

Computer news

How Facebook's "public search listing" could empower users



With news that Facebook is adding a public-facing (i.e. no need to log-in) "people search" function, that — in approximately one month's time — will be "spidered" by public

search engines, including Google, it's clear that the so-called social utility is one step closer to reaching its ambition to become an operating system for the social web.

The new "public listing search" feature enables anyone to search by name for a person on Facebook, which is sure to raise privacy concerns and test the social network's ability to balance "privacy" as a unique selling point, with the need to fine ever greater ways of driving traffic to the site and exploit all of the personal data that its persuaded users to volunteer.

To that end, the "public search listing" comes with a number of additional privacy controls:

The "public search listing" of a profile shows the profile picture thumbnail and links to interact with a user on Facebook.

People will always have to log in or register to poke, message or add someone as a friend. A user can also restrict what information shows in their public listing by going to the search privacy page. For instance, if a user does not want their profile picture to be shown, they can uncheck that box under "What people can do with my search results".

Additionally, users can choose to opt out of having their "public search listing" be indexable by external search engines — they'll have around a month to do so.

In relation to Facebook's latest move, Om Malik raises two interesting points. Where does this leave dedicated people search engines, such as the heavily funded Spock? and, how does this contribute to the growing problem of "digital

litter" in which people are leaving crumbs of personal information all over the web, in a way that makes it very difficult to Hoover up at a later date, if they so desire.

On the first issue, if Facebook continues to grow and eat into the social functionality of other web services, then people search could end up, largely, meaning Facebook profile search. Were that to happen then Spock et al. could be left in the dust. On the other hand, by making public profiles on Facebook indexable, might it actually help competing people search engines as they can now legitimately spider Facebooks data?

The issue of "digital litter" is a far bigger one than Facebook alone. And users may worry about their privacy even more, now that Facebook is publicly searchable. However, perhaps more worryingly is the way that users have been lulled into a false sense of security with regards to how these social networks (Facebook is not alone) invite users to volunteer and share so much information, much of which then ends up in Google's index, where there exists virtually no accountability or control.

Within this context, does Facebook's "public search listing" make the situation worse? I'm going to say no. Let me explain why.

Facebook results will inevitably end up pretty high in Google's index, so a search for my name through Google — were I to opt in — would probably bring up my Facebook profile before many of my other social web presences, let alone what others have written about me. Presuming this works out to be the case, the end result is that I now have more control over what "digital litter" you see first, because I can edit my profile any time I like, and the search engine will re-index the results. In other words, I now at least have a chance to influence how I'm represented on Google and online in general.

Submitted by: Greg.

My husband and I divorced over religious differences. He thought he was God and I didn't.

[Go to the top of this page](#)

AMD fans the flames with Barcelona pricing



The drumbeat for Barcelona is getting louder and louder. Advanced Micro Devices is widely expected to launch the new processor on Sept. 10—next Tuesday—at

speeds of up to 2GHz in a number of cities across the world, including San Francisco and Barcelona, of course (link: [here](#)). AMD has confirmed that the quad-core processor has begun shipping for revenue (link: [here](#)), meaning customers are purchasing it in order to build inventories before launching products.

Now reports are saying AMD has communicated Barcelona pricing to its partners. DailyTech (link: [here](#)) is reporting that Opteron/Barcelona 2300 series processors will start at a list price of \$206, while Barcelona 8300 series processors will start at \$688.

If those prices seem a little low, that's because they are. But AMD is not intentionally discounting the pricing of the Barcelona chips discussed by DailyTech. Instead, what the chipmaker is doing is leaving room for the introduction of faster and thus higher model number processors later this year and into 2008. Taking a closer look, the \$206 list price of the entry-level 1.7GHz Opteron model 2344 HE, cited by DailyTech, carries a \$32 or roughly 15% premium over the current entry-level dual-core Opteron HE model 2210, which lists for \$174 on AMD's site, and runs at 1.8GHz.

If the premium—say 15%, using my one example—seems small, it's actually not. Due to competition between them, AMD and Intel often introduce new generations of processors at prices that are no more than current-generation processors. AMD did so when it introduced its second generation of dual-core Opterons. The fact that AMD will ask for more for Barcelona Opteron, and presumably its Phenom chips as well, underscores its confidence in the processors' performance. AMD, which has been struggling financially during 2007, could use a pricing

bump. Although AMD's third-quarter Barcelona shipments are likely to be small in numbers, the chip could influence the chipmaker's fortunes in the fourth quarter, for which it has said it aims to report a profit.

Submitted by: Greg.

Bogus-drug peddlers thrive online



Harry Lime, peddling diluted penicillin in post-war Vienna in the 1949 film *The Third Man*, was an early pioneer: Today the counterfeit medicine business has gone global, fueled by the "perfect channel" of the Internet, according to a U.N. drug watchdog.

In many countries, the abuse and trafficking of prescription drugs, including stimulants and painkillers, now equals or exceeds the use of illicitly manufactured heroin, cocaine, amphetamine and opioids, according to the Vienna-based International Narcotics Control Board (INCB).

In the United States, it is second only to cannabis.

The massive demand for these drugs--together with lifestyle medicines such as Pfizer's *Viagra*--has led to an explosion in counterfeits, sometimes with fatal results.

"The sophistication of the counterfeiters certainly has increased tremendously," Gisela Wieser-Herbeck, a drug control officer at the INCB, told Reuters.

"It's a market where you can make a lot of money," she added.

The human cost can be devastating. Victims include women in Argentina who died after taking a bogus anemia treatment, deaths in Cambodia due to fake malaria drugs, and children in Haiti and India killed by paracetamol made with antifreeze.

In many African countries and parts of Asia and Latin America more than 30 percent of medicines

[Go to the top of this page](#)

(Continued on page 4)

on sale may be counterfeit, according to the World Health Organization (WHO).

Most industrialized countries have a fake drug rate of less than 1 percent, although a recent spate of fake cholesterol, schizophrenia and cancer drugs in Europe has raised concerns that criminals are spreading their net.

The INCB, which will address the problem at its next session in November, has called on governments to do more to enforce existing legislation. But tackling the criminal trade is difficult.

"The Internet provides a perfect channel because there is no national control mechanism, there is no quality assurance, and there is nobody who is going to ask where you got the supply," Wieser-Herbeck said.

Properly regulated, Internet pharmacies can provide a valuable service by increasing competition and offering access to treatments in underserved areas.

But all too often the online world is a Wild West of spam e-mails and hard-to-trace suppliers.

A global survey last month by U.S.-based brand protection firm MarkMonitor found only four of 3,160 online pharmacies studied were accredited as Verified Internet Pharmacy Practice Sites, the industry standard.

And average prices for six top-selling drugs on the non-accredited sites were 75 percent cheaper than on approved ones, suggesting most products were dubious.

Wieser-Herbeck said many bogus drugs appeared to originate in Asia, especially China, whose image has been badly tarnished recently by a range of product safety scares.

In July, China executed its former head of the State Food and Drug Administration for corruption and dereliction of duty. Later the same month, 15 members of a crime ring were arrested for selling fake drugs, including a counterfeit rabies vaccine.

Study: Cell phones, hospitals don't mix



Using mobile phones near hospital beds or important equipment is dangerous and could switch off ventilators or disrupt pacemakers, Dutch researchers said on Thursday.

The University of Amsterdam researchers recorded nearly 50 incidents of electromagnetic interference from cell phone use in hospitals and classified 75 percent of them as significant or hazardous.

Because of this mobile phones should come no closer than one meter to hospital beds and equipment, said the researchers who published their study in BioMed Central's online open access journal Critical Care.

"Critical care equipment is vulnerable to electromagnetic interference by new-generation wireless telecommunication technologies with median distances of about 3 centimeters," they wrote.

The study contradicts a study earlier this year from researchers at the Mayo Clinic who found that 300 tests over a five-month period turned up no noticeable interference with important hospital equipment due to regular mobile phone use.

The Dutch team--which tested 61 different medical devices--found that most of the incidents stemmed from the latest General Packet Radio Service signal, a new-generation technology that allows things such as wireless Internet access.

Other malfunctions they attributed to electromagnetic interference included complete stops with no alarms in syringe pumps and incorrect pulsing by an external pacemaker.

Submitted by: Greg.

I don't suffer from insanity; I enjoy every minute of it.

New chip promises to track kids from miles away



A technology originally developed to help the military track operatives in the field may in the next few years be used by parents to find kids in an amusement park.

Gentag will try to commercialize what it calls a Radar Response Tag, which effectively acts as an accurate homing beacon. In field tests, the tag can track someone more than 12 miles away and pinpoint their location within 3 feet, said Gentag founder John Peeters in an interview.

Twelve miles far exceeds the capabilities of conventional radio frequency ID (RFID) chips. The signal range of those chips is measured in feet. The longer-range global positioning system reaches farther, but the radar response system can track people through walls and other environmental obstacles.

"GPS is extremely accurate, but it doesn't work inside buildings," Peeters said. "You can think of this (radar response) as sort of super RFID."

Gentag will market the system as a way to keep track of kids or elderly relatives. It will also be pitched at hikers and campers. The system can piggyback on existing wireless infrastructures, Peeters added.

The technology is the outgrowth of a military project kicked off in 1990. The military wanted a better way to track soldiers without getting interference from leaves or buildings, so it commissioned Sandia National Laboratories to develop a solution. Seven years later, Sandia came up with the radar response system. The system works at the 430 megahertz frequency, Peeters added.

"The military uses it for friendly-fire avoidance," he said.

Sandia has now licensed its interest in the technology to Gentag. Mike Lovejoy, who helped develop the tag at Sandia, will work with Gentag to commercialize the technology.

Because the military has been using the technology for years, much of the field testing is already accomplished. Gentag now hopes to fine-tune the consumer product and come out with credit-card-size devices that would exchange signals between each other. Ultimately, Gentag would like to cut deals with phone makers to incorporate the chips into cell phones.

Employing chips to track the locations of individuals has generated controversy in recent years. Many have objected to the plans of some companies to implant RFID chips into individuals. On the other hand, one of the hot consumer items in Japan is a portable GPS device with an emergency button. Push it, and private security firms track down the recipient. Parents buy it for their kids.

Submitted by: Greg.

Who launched that attack?



Commentary--Mass e-mailing is no longer hip for hackers. Spam attacks are now yesterday's news and have been replaced with targeted attacks. There are two predominant reasons for the switch:

First, mass mailing malware is noisy and slow; it typically takes considerable time for an e-mail to work its way across the Internet. This global lag provides administrators with ample time to notify users and lock down the network to mitigate the attack.

Second, using a broad and unqualified e-mail address list may generate a few hits for a hacker--but for the most part it delivers lots of misses. Simply put, if the malware launcher wants to capture banking credentials with a key logger, he would be better served to only target users who have high balances in their bank accounts.

A recent report from Gartner clearly shows that the bad guys have, in fact, become much more targeted. Gartner found that if you earn more than \$138,000 per year, you will receive

50 percent more spam, and higher income individuals tend to lose more money when they fall for a scam as well. For example, if you earn less than \$138,000 and fall victim to phishing, the average loss is \$1,500, while those earning more than \$138,000 lose \$5,700 on average.

So how do attacks begin and evolve? Let's take a look.

First a BBB phishing Trojan

The most recent example of this was a phishing scam that started as a targeted attack against executive-level managers. The mass e-mail included a subject line indicating the message contained a consumer complaint from the Better Business Bureau (BBB). If a recipient clicked the attachment, a sophisticated Trojan was installed on the recipient PC that stole all interactive data sent from the recipients' web browser to a compromised web server.

Morphed into IRS phish

As with the BBB e-mail, a new version of the phishing Trojan was disguised as a criminal investigation notice from the IRS. This was also a targeted attack against executive-level managers and contained a similar—if not identical—malware payload. When the user clicked the attachment, a sophisticated Trojan was installed on the recipient PC that stole all interactive data sent from the recipients' Web browser. With the IRS e-mail, the malware launcher set up a new server to receive the stolen information that was registered to a domain in China. The server was also physically located in China.

Reverted back To BBB Trojan

The second time around, the e-mail scam used a domain called "business-complaints.com," registered in China. This second version was thought perhaps to be a more convincing message due to the domain name.

Change in tactics: FTC camouflage

In this scam, hackers used a spoofed FTC e-mail address designed to convince the recipient that someone had filed a complaint against them. A copy of the complaint was attached to the e-mail—but the attachment contained the Trojan. Again, the e-mail targeted executive-level managers. When the recipient clicked to

[Go to the top of this page](#)

view the attachment, a sophisticated Trojan was installed on the recipient PC. Next, the Trojan stole all interactive data sent from the recipients' Web browser.

New "proforma invoice" disguise

The current version of the scheme is still operating as a targeted attack aimed at executive-level managers and is again using a Trojan. The Trojan steals all interactive data and sends it from the recipients' web browser to one of three domains: (1) www.hlplace.com, (2) www.tanzatl.org and (3) www.aecv.ch. This scheme uses so-called social engineering-- which is the hacking of a normal human process or occurrence. Specifically, this scheme uses a Proforma Invoice, the receipt of which, by a senior level manager, is not an uncommon occurrence.

So, who's behind these schemes? There is some disagreement within the research community. Some researchers believe there is a single group of coordinated hackers at work. Others think competing groups are each learning from the others' success and adding the new wrinkles to the next variant of the scam. Most believe the Trojans send stolen information to China either through servers registered and located within China or through compromised servers in other countries thought to be controlled by Chinese hackers.

As of June 2007, only a small number of anti-virus vendors were able to detect the payload of the Proforma Invoice e-mail as being malicious. For unsuspecting users, these e-mails are quite well written. They typically include a plausible subject line and a well-socially-engineered message.

Since these are very targeted messages rather than bulk spam blasts, anti-virus will not be able to detect the payload and this scam will likely be one of the most profitable in recent memory.

Submitted by: Greg.

Don't take life too seriously; No one gets out alive.

Office Hours: The Top 7 employee bungles using Office



Even Microsoft employees are not immune from the everyday pitfalls and mistakes that everyone is bound to make at work. Read Philip Su's hilarious take on how some of us Office "experts" make the same mistakes our customers do ... over and over again.

The last type of question is by far the most common, especially with the airport crowd. But these strangers base their questions on a critically-flawed premise: They assume that Microsoft employees actually know how to use Microsoft products.

So without further ado, and to show you that we struggle with technology just like everyone else, here are the Top 7 Microsoft Employee Bungles using Microsoft Office that I've witnessed.

Top 7 employee bungles using Office

1. Opening dangerous attachments. Viruses like Melissa ("I love you!") were a huge problem at Microsoft. The kicker about it is that everyone acted flabbergasted and incredulous. "What sort of idiot clicks on these things?!" It's like Hootie and the Blowfish: the best-selling debut album of all time has no fans. Have you ever met a single person who admitted to owning Cracked Rear View? Same with Melissa.

2. Forgetting to include attachments. This is the evil twin of #1: in addition to clicking on harmful attachments, we forget to include useful attachments. So when you see an email with the subject "Foolproof Plan for World Peace — Part Deux," don't get too excited. As awesome as the plan probably is, it's almost definitely not attached to the email.

3. Replying-all to huge mailing lists. Any email to a large alias inevitably results in someone (no doubt a proud Hootie CD owner) replying to everyone. The threads are always the same. Something rather mundane or obscure is sent to thousands of people. Then the fan mail starts pouring in:

- "Why am I on this list?"
- "Unsubscribe."
- "Please also remove me!"
- "Please stop replying to everyone — there

are thousands of people on this alias."

- "Me too!"
- "SERIOUSLY — STOP REPLYING ALL!"
- "Why are you shouting?"
- "We never talk anymore."

The most famous of these threads at Microsoft started on a mysterious distribution list called "Bedlam DL3." 25,000 employees, 15.5 million e-mails, 195 GB of bandwidth, busted network. T-shirts were printed to commemorate the event.

4. Putting aliases in the "To:" field in order to see who's in them. To see names on an alias, you can put the alias in the "To:" field of an email and double-click it ... if you're a complete idiot. A friend of mine ("Jimmy") almost got fired by an executive for doing this. A product that this executive was in charge of was getting cancelled, but her team didn't yet know it. When Jimmy heard the scoop, he wrote his boss an e-mail that essentially said, "Hey there, so-and-so's team is getting canned. Here are the only three people worth keeping..." He then proceeded to add so-and-so's entire team to the "To:" line in order to find out the names of the "only three people worth keeping." The rest of what happened is left as an exercise to the reader.

5. Projecting a PowerPoint presentation. The amount of time wasted at Microsoft sitting in conference rooms waiting for the presenter to get the slides to work is mind-boggling. Does the projector handle your resolution? Press Fn-F5! Click the little icon in the lower left to resume your slide show. Not that icon! The other one! Oh, the screen saver's kicked in. Your laptop's suspending!

6. Getting instant messages (IMs) during presentations. Once the presentation is going, IM notifications inevitably pop up on the screen. This tends to happen most when you're presenting in front of hundreds of people. "Yo! How did the [blind-date/colonoscopy/armed-robbery] go?" "Hi, [term of endearment]! I can't wait to [verb] your [adjective][noun] [now/tonight/again/forever]!" I'm told that the latest version of Office fixes this. Let's hope so.

NOTE From the Editor: In 2007 Office system, Desktop Alerts for incoming e-mail messages are turned off by default when you run a PowerPoint 2007 presentation. See Turn Desktop Alerts on or off for more info.

[Go to the top of this page](#)

(Continued on page 8)

7. Using Excel to cover up Unreal Tournament. Well, I've only seen this once, but it's so eponymous that it deserves to be celebrated. A few years ago, one of my team members frantically maximized Excel as I walked into his office. As I began discussing a technical issue with him, sounds of gunfire, grenades, and general human suffering erupted from his speakers. I had a difficult decision to make while recovering from my brief initial confusion: Do I acknowledge what was already mutually embarrassing and awkward, or do I ignore the obvious? I decided to conduct our technical discussion with the idyllic calm of a wartime correspondent. To his credit, I now know that should push come to shove, my team member could calmly discuss a spec during Armageddon without batting an eyelash.

As you can see, Microsoft employees are often just as befuddled as everyone else. It would blow your mind if you could hear how frequently basic Office tips are shared in my hallway at work. Spend a day here, and you'll find it impossible to believe that we're all Office mavens marching lockstep towards a streamlined plan for world dominion.

Then again, Office 2007 is far easier to use. I'm impressed by the many improvements in its user interface. So in a funny way, perhaps we're no longer as harmless as we used to be. World dominion may be within our grasp after all.

If we could only remember to attach our plan in email...

Submitted by: Greg.

I used to have a handle on life, but it broke

Microsoft updates Windows without users' consent



Microsoft has begun patching files on Windows XP and Vista without users' knowledge, even when the users have turned off auto-updates.

Many companies require testing of patches before they are widely installed, and businesses in this situation are objecting to the stealth

patching.

Files changed with no notice to users

In recent days, Windows Update (WU) started altering files on users' systems without displaying any dialog box to request permission. The only files that have been reportedly altered to date are nine small executables on XP and nine on Vista that are used by WU itself. Microsoft is patching these files silently, even if auto-updates have been disabled on a particular PC.

It's surprising that these files can be changed without the user's knowledge. The Automatic Updates dialog box in the Control Panel can be set to prevent updates from being installed automatically. However, with Microsoft's latest stealth move, updates to the WU executables seem to be installed regardless of the settings — without notifying users.

When users launch Windows Update, Microsoft's online service can check the version of its executables on the PC and update them if necessary. What's unusual is that people are reporting changes in these files although WU wasn't authorized to install anything.

This isn't the first time Microsoft has pushed updates out to users who prefer to test and install their updates manually. Not long ago, another Windows component, svchost.exe, was causing problems with Windows Update, as last reported on June 21 in the Windows Secrets Newsletter. In that case, however, the Windows Update site notified users that updated software had to be installed before the patching process could proceed. This time, such a notice never appears.

For users who elect not to have updates installed automatically, the issue of consent is crucial. Microsoft has apparently decided, however, that it doesn't need permission to patch Windows Updates files, even if you've set your preferences to require it.

Microsoft provides no tech information — yet

To make matters even stranger, a search on Microsoft's Web site reveals no information at all on the stealth updates. Let's say you wished

[Go to the top of this page](#)

to voluntarily download and install the new WU executable files when you were, for example, reinstalling a system. You'd be hard-pressed to find the updated files in order to download them. At this writing, you either get a stealth install or nothing.

A few Web forums have already started to discuss the updated files, which bear the version number 7.0.6000.381. The only explanation found at Microsoft's site comes from a user identified as Dean-Dean on a Microsoft Communities forum. In reply to a question, he states:

§ "Windows Update Software 7.0.6000.381 is an update to Windows Update itself. It is an update for both Windows XP and Windows Vista. Unless the update is installed, Windows Update won't work, at least in terms of searching for further updates. Normal use of Windows Update, in other words, is blocked until this update is installed."

Windows Secrets contributing editor Susan Bradley contacted Microsoft Partner Support about the update and received this short reply:

§ "7.0.6000.381 is a consumer only release that addresses some specific issues found after .374 was released. It will not be available via WSUS [Windows Server Update Services]. A standalone installer and the redistributable will be available soon, I will keep an eye on it and notify you when it is available."

Unfortunately, this reply does not explain why the stealth patching began with so little information provided to customers. Nor does it provide any details on the "specific issues" that the update supposedly addresses.

System logs confirm stealth installs

In his forum post, Dean-Dean names several files that are changed on XP and Vista. The patching process updates several Windows\System32 executables (with the extensions .exe, .dll, and .cpl) to version 7.0.6000.381, according to the post.

In Vista, the following files are updated:

1. wuapi.dll
2. wuapp.exe
3. wuauclt.exe
4. wuaueng.dll
5. wucltux.dll
6. wudriver.dll
7. wups.dll
8. wups2.dll
9. wuwebv.dll

In XP, the following files are updated:

1. cdm.dll
2. wuapi.dll
3. wuauclt.exe
4. wuauclt.cpl
5. wuaueng.dll
6. wucltui.dll
7. wups.dll
8. wups2.dll
9. wuweb.dll

These files are by no means viruses, and Microsoft appears to have no malicious intent in patching them. However, writing files to a user's PC without notice (when auto-updating has been turned off) is behavior that's usually associated with hacker Web sites. The question being raised in discussion forums is, "Why is Microsoft operating in this way?"

Submitted by: Steve Wawrykow

These two articles are related to the previous article and they are too big to put in the newsletter. So I have attached them

[Protect yourself from silent Windows updates](#)

[Stealth Windows update prevents XP repair and how to fix it](#)

Submitted by: Steve Wawrykow

Beauty is in the eye of the beer holder.

Microsoft pushing Office 2007 with promos galore



Office 2007 is selling like hotcakes, according to the market researchers at NPD. And one big reason is the try-before-you-buy program that Microsoft put in place when it launched the product.

But promotions and steep discounts also could be another reason behind Microsoft's success with Office 2007.

On August 1, Microsoft launched a new incentive program called the "Office Partner Services Subsidy Promotion." The promo runs until January 31, 2008. To take advantage of it, customers must purchase a minimum of five and maximum of 200 qualifying Open volume licenses for Office Enterprise 2007, Office Professional Plus or Office Small Business. With each copy of Office purchased under the program, customers get up to a \$150 partner subsidy that they can spend on software, hardware and/or services from their preferred partner.

Meanwhile, at the lower end of the market, Microsoft is kicking off on September 12 a promotion aimed at moving copies of Office 2007 Ultimate. Students can obtain a copy of the latest Office suite for \$59.95. The normal retail price of this SKU is more than \$600. The offer ends on April 30, 2008.

(Ironically, given Microsoft's growing crackdown on software piracy, the student promotion is named "The Ultimate Steal.") Here's Microsoft's official release on the Office-student program, which it issued on September 12.

There just don't seem to be as many high-visibility Vista promotions out there as Office ones. Maybe if there were, the retail sales numbers for shrink-wrapped copies for Vista wouldn't be quite so bad.... Anyone know of any Vista deals worth checking out for those who've decided to upgrade?

Submitted by: Greg.

Earth is the insane asylum for the universe.

One-year-old QuickTime bug comes back to bite Firefox



A year ago this month, security researcher Petko D. Petkov (left) released details on vulnerabilities in Apple's QuickTime media player to show how movie and MP3 files can be backdoored to hack into Firefox.

Apple fixed one of the bugs but the second issue, which allows malicious manipulation of QuickTime Media Link (.qtl) files, remains unpatched and presents a serious danger to Firefox users.

According to Petkov, a U.K.-based penetration testing specialist, the result of this vulnerability can lead to full compromise of the browser and maybe even the underlying operating system.

In a blog entry that includes several proof-of-concept exploits, Petkov said the flaw can be used to install browser backdoors and take control of the underlying OS if the victim is running with administrative privileges.

I attempted to test some of the demo exploits (Firefox 2 on Mac OS X) and got this warning from Firefox:

However, on a fully patched Windows XP SP2 machine running Firefox 2, one of the exploits launched calc.exe without warning: Because QuickTime is installed by default alongside iTunes, Petkov warns that iTunes users are also at risk.

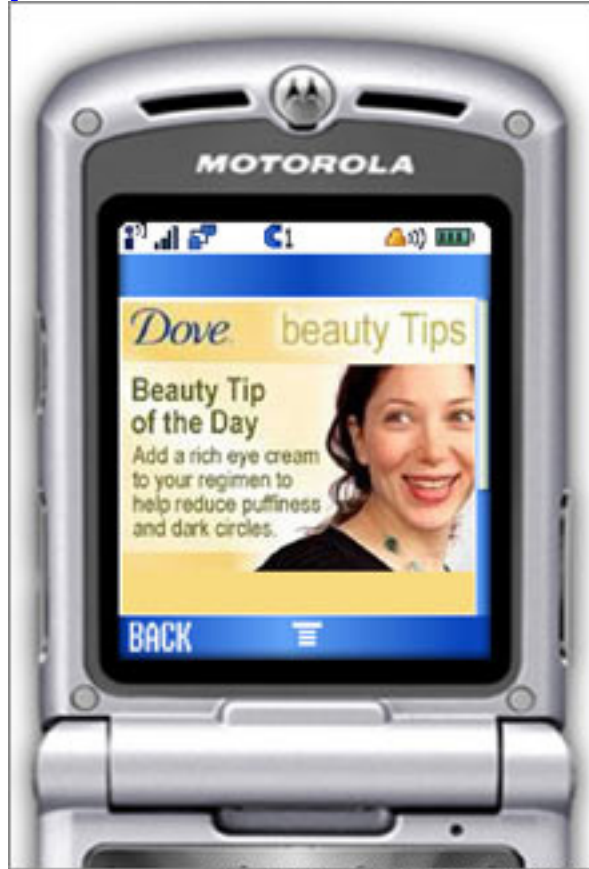
Apple does not respond to queries on individual security issues. So far this year, the company has shipped at least five QuickTime/iTunes security updates but Petkov's one-year-old disclosure is still unpatched.

ALSO SEE:

Serious QuickTime bugs bite Windows Vista, Mac OS X

[Go to the top of this page](#)

Get ready for ads on your cell phone



COURTESY: THIRD SCREEN MEDIA

QuickTime bug brought down MacBook

[UPDATE: September 13, 2007 at 8:33 AM] Mozilla security chief Window Snyder has confirmed this is a "very serious issue" for Firefox users. "[We are] working with Apple to keep our users safe and we are also investigating ways to mitigate this more broadly in Firefox.

If Firefox is the default browser when a user plays a malicious media file handled by Quicktime, an attacker can use a vulnerability in Quicktime to compromise Firefox or the local machine. This can happen while browsing or by opening a malicious media file directly in Quicktime. So far this is only reproducible on Windows.

Firefox security response team is working on a fix but there's no explanation as to why it took the two companies a full year to pay attention to Petkov's warnings.

Submitted by: Greg.

A little boy was attending his first wedding.

After the service, his cousin asked him, "How many women can a man marry?"

"Sixteen," the boy responded. His cousin was amazed that he had an answer so quickly.

"How do you know that?"

"Easy," the little boy said.

"All you have to do is add it up, like the pastor said,

4 better, 4 worse, 4 richer, 4 poorer."

Your cell phone may be one of the last spots around that's relatively free of advertising--but not for long. Media and advertising companies have found a way of latching on to people's handsets by beaming ads to them via Bluetooth, the same technology used in some hands-free headsets.

Here's how it works: When you're standing less than 10 meters away from a Bluetooth interactive billboard, window display or concert hall booth, you'll be asked if you want to switch on your Bluetooth function and accept a file. That file could be a video, a song or an offer of rebate coupons.

As you are strolling down the Champs Elysees, for instance, don't be surprised if one day Lancome, using the technology, invites you to test its newest perfume in a nearby shop. You may also find yourself on the receiving end of ad clips from Coca-Cola or a Warner Bros. preview of its Happy Feet animated film.

"A mobile phone is the one electronic device

[Go to the top of this page](#)

most people carry with them at all times, so it is too good of an opportunity for media companies and advertisers to miss," says Nick Jones, wireless technology analyst at Gartner research house.

But cellular phone operators aren't showing much enthusiasm for Bluetooth marketing since it's free for the consumer and often does not generate extra revenues for them.

Instead, mobile operators such as Orange favor a rival technology to Bluetooth called Code 2D-or QR (quick response codes).

These bar codes, already used in Japan, are read by camera phones and send the user directly to a Web page. Accessing a Web site requires a subscription to a wireless Internet connection for which users usually have to pay.

"Bluetooth does not answer all our needs for mobile marketing," Jean-Noel Tronc, head of Orange Mobile in France, told Reuters in an interview. "For us, Code 2D is much better."

Orange, which also operates in the U.K., Poland and Spain, has asked manufacturers--starting in early 2008--to supply it with camera phones with Code 2D capabilities.

But advertisers don't necessarily need the support of operators. After all, consumers can use Bluetooth to download files regardless of which operator they have chosen, or even without one.

So don't be surprised if Bluetooth ads become commonplace down the road. After all, they allow for better targeted and more relevant advertising than mass media like television or radio.

"Mobile marketing is a one-to-one relationship, while TV or radio marketing is one-to-many," says Gartner's Jones. "Mobile phones take this personalized form of marketing a step further."

Something else to take into account with such marketing is whether it will simply annoy consumers.

Fabien Beckers, CEO of Paris-based mobile

[Go to the top of this page](#)

marketing firm Kameleon, rejects the idea that such ads are just spam, since consumers receive them only on an opt-in basis.

Still, most agree that for Bluetooth marketing to work, consumers need to get something out of it. The picture of an insurance company's logo probably won't attract much interest.

"(Mobile marketing) has the potential to become a significant player in the marketing world as TV advertisers struggle to get people's eyeballs," says Jon Hudson, senior vice president of PC, automotive and consumer business units at CSR, "But it has to be more than 'your next McDonalds is 200 meters on the left.'"

Some local authorities believe Bluetooth proximity communication has a future in the public services arena as well.

This month Paris City Hall has started offering maps and updated what's-on guides beamed from 20 of the city's self-hire bike stations, which have been all the rage since they were installed in July.

"We are trying to test the public's ability to use Bluetooth and their appetite for such 'take-away' information," says Jean-Philippe Clement, the Paris City Hall IT official who oversees the bike station Bluetooth project.

Submitted by: Greg.

God must love stupid people; He made so many.

How law enforcement uses Google Earth



When a Wisconsin man was arrested last October on suspicion of harvesting 18 pounds of marijuana, it was partly thanks to Google Earth.

The sheriff's deputies who pulled the man over found, in addition to what they estimated was at least \$63,000 worth of pot, a GPS unit around his neck that was filled

with a series of local coordinates, according to The Journal Times of Racine, Wis. After plugging those coordinates into Google Earth, the police were able to identify the location of several marijuana fields to which the man was allegedly connected.

While the cops would have been able to find the fields strictly based on the GPS coordinates, their use of Google Earth demonstrated just one way in which law enforcement agencies across the country and around the world are using the popular mapping service, both to fight crime and to offer valuable information to the public.

It's impossible to say just how many law enforcement agencies are actively using Google Earth, but one thing is certain: looking at Google's often detailed images is a lot cheaper than flying helicopters or planes, particularly in remote areas with cash-strapped police departments.

Todd Fulton, a deputy in the Humboldt County, Calif., sheriff's department, said his agency is also using Google Earth as one piece in its marijuana interdiction activities, albeit a small one. "We'll use GPS (devices) and transfer the GPS data over to Google Earth," Fulton said, "to get an idea of the terrain we're dealing with."

That's particularly useful in a region like Humboldt County--one of the largest marijuana-growing regions in the United States--given that it consists of millions of acres of rough, hilly terrain. So being able to use Google Earth to do something that previously might have required flying around in a helicopter is much more efficient, Fulton suggested.

Of course, given the realities of Google Earth, it's unlikely that law enforcement would ever be able to use the service as the sole means of interdiction, despite the high degree of visibility it gives them.

One Northern California marijuana grower contacted for this story said that using Google Earth, he is able to see the exact location on his property where his plants are growing. But he's not worried that the police will be raiding his land any time soon.

"You would have to be really well-versed in the whats and wherefores," the grower said, "to be able to identify my (growing operation). My game is really well-observed."

Chuck Herring, director of communications for satellite data provider DigitalGlobe, said he thinks that the quality of the imagery his company offers, and that of Google Earth, is good enough to spot things like large marijuana fields.

But the bigger problem, according to Herring, and to Frank Taylor, who runs the unofficial Google Earth blog, is that the images from the mapping service are not timely enough for police to use for law enforcement activity.

"I think it's useful, but there are some caveats," Taylor said. "The satellite photography in Google Earth is not live. It's not even recent. In most cases, it varies widely from as recent as a few months old to a few years old."

Taylor said some law enforcement agencies have access to the enterprise version of Google Earth, which may have more recent photography. Still, it's not likely that even that data would help police nab pot growers in the act.

Beyond pot busts

But several agencies have found other ways to utilize the service, both for law enforcement and for public service. He explained that there have been multiple cases of tax authorities using Google Earth to crack down on homeowners who have built additions to their property but who are not paying taxes on that new construction, Taylor said.

They've "begun using Google Earth imagery to help identify property builder violations where (people have) added onto their houses without reporting it," said Taylor, "and they've been using that to get them to pay tax penalties." Authorities can compare the satellite imagery to existing records and see where additions have been made illegally.

A more public service-oriented utilization of Google Earth by law enforcement is one undertaken by the Ohio State Highway Patrol. For the past two years, the agency has been

providing Google Earth data showing the locations of fatal accidents--including those identified as being alcohol-related. The agency is also providing data showing the locations with the highest frequency of drunk-driving arrests.

Using that data, it's possible to get a sense of dangerous roads or intersections, including those on which people are more likely to be driving drunk, Taylor said.

"You can see where more drunk drivers have been found," Taylor said. "Those are places you might want to avoid on a Saturday night."

At the same time, some Google Earth users have found a way to use the service that law enforcement probably wishes they weren't. One database shows the location of hundreds of speed cameras--those used by police to automatically catch people speeding--all over Western Europe.

"It's one of the most popular (plug-ins) in all of Europe," Taylor said. "I can't imagine why."

Submitted by: Greg.

Consciousness: That annoying time between naps.

Gmail cookie vulnerability exposes user's privacy



Petko Petkov of "ethical hacking" group GNUCitizen has developed a proof-of-concept program to steal contacts and incoming e-mails from Google Gmail users.

"This can be used to forward all your incoming e-mail," Pure Hacking security researcher Chris Gatford said. "It's just a proof of concept at the moment, but what they're demonstrating is the potential to use this vulnerability for malicious purposes."

According to Gatford, attackers could compromise a Gmail account--using a cross-site scripting vulnerability--if the victim is logged in and clicks on a malicious link. From that moment, the attacker can take over the session

cookies for Gmail and subsequently forward all the account's messages to a POP account.

"If someone picks up on this before Google fixes it--or if someone knew of the vulnerability before this guy published it--this could be very damaging to Gmail users," he added.

The problem is potentially compounded by Google's policy of retaining cookies for two years.

"Once you've managed to snarf a cookie, you can access (a user's) Gmail account without the password for the next two years," he said.

While the obvious risk is to the home user, many organizations could be exposed, since they do not filter employee e-mails sent from work to personal accounts, he added.

"People do use private accounts to store work information," IBRS security analyst James Turner said. "I've worked at one organization where this was implicitly expected, because the mail server at the time was so unreliable. But that scenario is certainly less than optimal."

"In an ideal world, an organization would be able to draw a line in the sand and say that corporate data does not pass this point. The current reality is that there are Gen-Y workers who are sharing information with each other on multiple alternative communication channels--Gmail and Facebook included."

One work-around is to use Gmail through Firefox and disable JavaScript. While this limits user access to many components of popular Web sites, it will protect against the potential threat.

Developers at many large enterprises are not aware of the power of cross-site scripting, said Pure Hacking's Gatford. "In the last year or so, (XSS vulnerabilities) have been used by attackers to grab cookie values and therefore gain access to normally password-protected sites."

"When you have organizations like Google spending countless man-hours reducing security vulnerabilities...you can imagine how bad the actual situation is for other organizations,"

[Go to the top of this page](#)

Gatford said.

Gatford advised organizations to use resources such as the Open Web Application Security Project, or OWASP, which offers free tools to help write secure code and allow testing for XSS vulnerabilities.

Google was unavailable to comment.

Submitted by: Greg.

Ever stop to think, and forget to start again?

Privacy experts: T.J. Maxx breach was foreseeable



The breach of sensitive personal information held by TJX, operator of discount chains including T.J. Maxx and Marshalls, earlier this year was foreseeable, but the company failed to put in place adequate security safeguards, according to a report.

"The company collected too much personal information, kept it too long, and relied on weak encryption technology to protect it, putting the privacy of millions of its customers at risk," Jennifer Stoddart, the privacy commissioner of Canada, wrote in the report, which was released Tuesday.

Modern crime made a large-scale breach of this kind inevitable, Stoddart concluded. "Criminal groups actively target credit card numbers and other personal information," she said in the report. "A database of millions of credit card numbers is a potential goldmine for fraudsters, and it needs to be protected with solid security measures."

What made such a breach more likely was that the information had been kept for a long time, she said. "The TJX breach is a dramatic example of how keeping large amounts of sensitive information, particularly information that is not required for business purposes, for a long time can be a serious liability."

Stoddart said the affair was a "wake-up call" for all retailers.

Frank Work, the information and privacy commissioner of Alberta, added: "They must collect only the personal information necessary for a transaction."

TJX disclosed in January that its computer system had been breached, putting millions of credit and debit card numbers as well as other personal information at risk. In May, TJX said it believed the hackers gained access to its information via the Wi-Fi networks.

Details of 45 million customers of TJX were put at risk. The company could offer no comment at the time of writing.

Submitted by: Greg.

DRM troubles drive ex-Microsoft employee to Linux



A security expert who once worked for Microsoft has said he may dump the company's Windows Media Center in favor of Ubuntu-affiliated LinuxMCE after struggling with the

software giant's digital-rights management software.

Jesper Johansson--a former senior program manager for security policy at Microsoft who moved to Amazon in September last year--wrote in his blog on Monday that he may drop Windows Media Center for LinuxMCE, a free open-source add-on to the Kubuntu desktop operating system, because problems caused by Microsoft's digital-rights management (DRM) software have proven so difficult to fix.

After Johansson's 5-year-old child complained that cable network Comcast's On Demand video system was not working with Windows Media Center, Johansson wrote, he attempted to resolve the problem.

"Upon inspecting the problem I found that the video would turn on, the screen would flicker

[Go to the top of this page](#)

for a second each of black and the video a few times, and then the Blue Screen of DRM came up. It also wouldn't play any premium channels," he wrote.

Johansson said the recommended work-around involved several convoluted steps, including installing Windows Media Player 10, which crashed, and then being advised to troubleshoot the problem with Windows SharePoint Services. A subsequent Microsoft DRM update then caused the Internet Explorer browser to crash.

Johansson said that DRM software is not only ineffective, but a waste of money that is damaging businesses attempting to use it to control the way consumers use copyright material.

"How many billions has the industry spent on DRM schemes that the bad guys break in weeks? How many perfectly legitimate users has the industry annoyed and driven away? How many lost DVD sales has it caused? How many lost sales of Microsoft's Media Center software and Windows Vista has it caused because the DRM subsystem randomly decides that you must be a criminal?" Johansson wrote.

DRM protections have done very little to stop bootleggers from hawking counterfeit software, he wrote, after witnessing a bustling trade in pirated material on a recent trip to Asia. Johansson wrote that he is now contemplating using LinuxMCE to avoid further difficulties.

Submitted by: Greg.

I used to have a handle on life, but it broke

Google eyes discreet Street View for Canada



Google is considering a Canadian launch of its Street View map feature, which offers street-level close-ups of city centers,

but would blur people's faces and vehicle license plates to respect tougher Canadian privacy laws, the Web search firm said on Monday. Canada's privacy commissioner told Google in

August that the feature--which offers a series of panoramic, 360-degree images of nine U.S. cities--could violate Canadian laws if it were introduced without alterations.

Some of the pictures feature people who can clearly be identified, which contravenes Canadian legislation on privacy.

"We are thinking about launching it outside the United States, including Canada, and we're looking at how it would have to be different in Canada compared to its U.S. version," said Peter Fleischer, Google's global privacy counsel.

"We would launch Street View in Canada in keeping with the principles and requirements of Canadian law ... that means we know we'll have to focus on finding ways to make sure that individual's faces are not identifiable in pictures taken in Canada and that license plate numbers are not identifiable in Canada," he told Reuters in an interview.

Google had been approached by a number of Canadian cities seeking to be featured, he said.

"(They) have said, 'Please come and start taking this imagery of our city. It's good for our tourist industry and we'll even pay you or reimburse your expenses to do so,'" he said.

Canada's privacy commissioner has yet to hear from Google, a spokesman said.

"If that's how they're planning to roll out their service by putting in place technological means ... to block out faces and license plates and other essential personal information, then that's a great first step," said Colin McKay.

The images of U.S. cities were produced in partnership with Canadian firm Immersive Media, which says it has taken similar street level pictures of major Canadian cities.

Fleischer said he did not know if the firm would be involved in any Canadian launch

Submitted by: Greg.

[Go to the top of this page](#)

This article is too big to put in the news letter. So I have attached it.

[Code Simple: E-mail encryption's becoming a snap](#)

Submitted by: Alan Forrest

Computer tips and tricks

Excel 2007 displays 65,535 as 100,000



Commenters in the microsoft.public.excel discussion forum revealed on Sept. 22 that Excel 2007 incorrectly displays floating-point numbers around 65,535 and 65,536 as 100,000. A

Slashdot user, however, reports that the affected cells work correctly in formulas and graphs, despite the errant display.

Microsoft blogger David Gainer acknowledged the problem on Sept. 25 and said the Redmond company is working on a fix. Until then, watch out when calculating those big mortgage payments!

Submitted by: Greg.

Prevent Internet Explorer From Saving Passwords



There may be times when it's necessary to clear your passwords in Internet Explorer 7. Here's how:

1) In Internet Explorer, open the Tools menu and click Internet Options

2) Click the Content tab in the dialog box, then click the Settings button and deselect the "User names and passwords on forms" checkbox

3) Click OK, and then click OK again.

Submitted by: Greg.

Being 'over the hill' is much better than being under it

The Dangers Of File Sharing - Lockergnome



Editors Note: While the first part of this refers to US Universities, there are many good points to be aware of with your children, if they are using file sharing programs

Q: My son is going to his first year at a major university and is an avid file swapping user. How concerned should I be about him getting into trouble at school if he continues using these questionable services?- Julian

A: File sharing networks that allow users to share songs, video, software or any kind of computer files got their start when a college student created a free program called Napster in 1999.

Napster allowed the students at that particular campus to quickly search other students' hard drives for specific songs and to download them once they were located.

This "peer-to-peer" sharing network eventually made it out to the Internet, which allowed millions of users to swap music files without having to pay.

What started out as a home grown project to allow 30 or so pals to share their music collection turned into a revolutionary way for anyone to share anything.

In February of 2001, the Recording Industry Association of America (RIAA) claimed that over 2.79 billion songs were traded during that month alone which all violated copyright laws and cost the music industry untold millions in revenue. (Ironically, Napster is now a legal music downloading service that has nothing to do with the student who created the original program.)

Our kids grew up with this technology, so most of them think that it's OK because "everyone does it." They see this unquestionably illegal activity as no different then speeding... it's only a problem if you get caught.

The problem for parents of avid file-swappers (and many parents have no idea that their children are engaging in this activity) is that they are sending their children right into one of the

[Go to the top of this page](#)

biggest targets of the RIAA; major universities. A survey last year suggested that 50% of college students engage in illegal file sharing and that's why the RIAA will continue to target universities. Last year over 15,000 complaints were filed by the RIAA at 25 schools, which led to punishment from the universities that ranged from stern e-mail warnings to semester-long suspensions. The RIAA also offered to "settle out of court" with those accused of illegal file swapping to avoid lawsuits and records. Press reports and attorneys that were involved with some of the cases estimated that the average settlement was around \$4,000.

The risk of using programs like KaZaa, LimeWire, eDonkey, WinMX, eMule or any of the BitTorrent software programs (a fairly comprehensive list is available here) has now gone way beyond the potential of just being caught by the RIAA.

Another major concern for anyone (not just college students) that participated in these file swapping networks is becoming a victim of identity theft or other malicious activity from cybercriminals.

The bad guys figured out how to get into millions of computers without a trace and post infected files that appear to be popular songs, movies, or software programs on file swapping networks. Once the file is downloaded and run, the hidden program can silently install itself onto the victim's system, while the victim thinks that they downloaded a "dud" file.

Any number of malware programs such as viruses, worms, Trojan horses, keyloggers (one of the favorite tools of the identity thieves), spyware, and adware can easily sneak into your system while you think you are getting away with downloading a movie or song for free.

If you want to see if your child has installed any P2P software, check your list of programs (Start/All Programs) or go to the Add/Remove option in the Control Panel and look at the list of programs that is currently installed (if you are not sure, get professional help - this one is too important to let slide!)

Parents need to add discussing this very real danger to all of the frank discussions they should have with their college-bound children as this one could cost both students and parents dearly if it is not taken seriously.

This article is too big to put in the news letter. So I have attached it.

[Internet Explorer 7 tools help you recognize phishing scams](#)