Computers and Stuff.

Sam Houliston.

Avoiding those unwanted free applications.

Windows Secrets

Free apps are great, but they often come with an unexpected cost, unwanted additional apps.

Depending on how you handle them, unwanted programs can be a minor annoyance, or a daunting problem. The trick is paying attention. These days, installing a free program can feel like running a gauntlet. You go to the program's webpage, click the big, colorful **Download** button … and end up with an entirely different program. You try again, only to discover you must download some sort of download manager to download the app you want.

Eventually, you install the intended software and heave a sigh of relief. But just as you're getting back to work, one or more unwanted apps mysteriously appear on your system, those really annoying browser toolbars, for example. You then waste more time removing the unwanted software and wonder whether that free program was worth the effort.

The perils of clicking free-download buttons.

Potentially unwanted software comes in many forms, from mainstream applications such as Chrome to annoying browser toolbars to really sketchy software that wants to ***fix*** your system. Many people simply refer to unwanted software as ***malware*****,** but that's a bit over the top. Yes, it often gets onto your computer in a sneaky manner and some versions do invade your privacy, noting your surfing and shopping habits for targeted advertising.

But in most cases, unasked-for software does nothing illegal. It's also reasonably easy to avoid and it can be uninstalled without resorting to an anti-malware tool. However, some unwanted software takes more work to remove than simply running an uninstaller. And occasionally, you discover you actually want the software!

Getting unwanted software typically begins at the download button. Consider, for example, **Eraser,** an excellent program that securely and completely deletes files. But take a look at Eraser's home page. See that big green **Download Now** button in the pic below, it doesn't download Eraser, nor do the other two big green download buttons further down the page. To get Eraser, you need to click the small, white-on-black Downloads link near the top. (Those green buttons are actually ads, and they change over time.)

A celebrity is a person who works hard all his life to become well known, then wears dark glasses to avoid being recognized.

Eraser page:
That big green Download button can easily trick you into installing an unwanted app.

Sometimes you have to download a downloader before you can download the program. This is now common on CNET's Download.com page, one of the most popular repositories of software on the Web. Many of the programs on the site don't download directly; the big green Download Now button delivers the CNET Download utility. It, in turn, downloads the software you want, after pitching something else.

Fortunately, CNET Download doesn't stay on your system after you've downloaded the desired software, however, it most definitely tries to download more programs than the one you wanted,

Eraser and Download.com are just two examples. But they're not by any means out of the ordinary, most free-download sites now do something similar. Your problems aren't over after you've finally downloaded the ***right*** program either. The app's installation wizard might have pre-checked offers for software someone wants on your computer. At this point, you need to be especially vigilant because the installation process might add unwanted software by default.

There's no such thing as a free application.

Why do application vendors make us jump hurdles for their free downloads? Just like you and me, software developers typically want to be paid for their time and effort. So they look for other ways to generate revenue for their products. Some apps, free anti-malware, for example, are supported by paid commercial or "professional" versions that can do more. In other cases, advertising is integrated into the user interface. Some products will track your Web surfing, gathering marketable information on your tastes and buying habits.

Or one software vendor will pay another to sneak its product onto your PC. And, surprisingly, it works for both parties. For example, MP3jam is a free, online, music-download service, one of the "Apps for building and organizing a music library." However, MP3jam will also install, by default, other programs you probably won't want. For example, it offers RealPlayer, (right) an app most Windows users don't need. According to an

MP3jam representative, "The revenue covers only one-third of our development and maintenance costs." They hope that will change: "As the number of installations rises, so does the revenue."

NCH Software's VideoPad Free app installs unwanted software if you don't uncheck an option. A company representative stated, "It's a good way to generate at least some revenue on a free program." But she also told me about customer confusion brought on by downloaders such as CNET's. The user might uncheck the option for a toolbar in the program's own installer but miss the one in the downloader then get angry at NCH for "ignoring" the user's choice.

OpenCandy manages the revenue and provides the code for adding third-party software offers to installers. When asked how much money a software developer can expect to make from the service, a spokesperson replied: "It varies from developer to developer, but some developers have made enough money to quit their day jobs."

The solution: Don't accept what you don't want.

You might now understand why software vendors add potentially unwanted software to their installers and you might even sympathize. But for most users, in almost all cases, the offers are simply more unwanted junk added to their PCs. Fortunately, you can install the apps you want without adding the uninvited apps. It just requires some care.

As noted above, it starts at the website. If there's a big bright Download button, don't automatically assume it's for the app you want. In fact, the bigger the button, the more likely it's trying to con you into downloading unwanted software. Before you click any button, carefully scan the rest of the webpage and look for other download links. Roll your mouse cursor over the button and see whether it behaves more like an ad. And when you click a button, check the file name before clicking **Save.**

Finally, examine the first page of the downloaded apps installation process to make sure you're installing the right program.

For sites that require downloading and running some form of download-management app, you have a few options:

- Obviously, it's always best if you can download an app from its developer's site.
- If it's a respectable, third-party site such as CNET's Download.com, it's usually safe to run the helper app. But read all the download/installation dialog boxes carefully, so you can uncheck every offer for unwanted software.
- Search the Web for other sites that offer direct downloads of the program. But again, be wary. If you don't know the site, the download file could be an out-of-date version of the app or contain real malware.

- Use a sandbox program such as Sandboxie to run the downloader. Then move the downloaded file out of the sandbox and run the installer.
- Find another program with similar capabilities to download and install.

During the installation process, keep a sharp eye out for any suspicious options. Installation options such as **Express, Default,** or **Typical** installation could mask the addition of unasked-for apps. Always select an **Advanced** or **Custom** install option, if offered. For example, iLivid's default installation setting automatically installs other, possibly unwanted, apps. You must use Custom installation to uncheck the extra apps.

If an unwanted app gets through and installs itself, it typically won't be a disaster. A mainstream application such as Chrome will have an uninstaller. Some browser toolbar add-ons can be more difficult to remove, but a quick Web search will in most cases provide a relatively easy solution.

Remember that the PC belongs to you (unless, of course, it's a company computer). You get to decide what goes onto it.

Don't let some freebie's installation routine make that decision for you.

God gave you toes as a device for finding furniture in the dark.

Outlook:
Strain out spam and safeguard senders.

Spam is such a looming presence in the world's email that you'd be hard-pressed to find a mail application that doesn't include some sort of spam management. Later versions of Outlook has some of the best.

If you use Outlook, here are the tools and techniques available to users for dealing with the onslaught.

Despite recent stories about major spam-sites being closed down, you've no doubt noticed that the number of unwanted messages filling your inbox is undiminished and improvements in spam filtering are, at best, just keeping up with a rising tide. According to a recent Kaspersky Lab report, spammers send about 70% of the entire world's email, and the number is rising. Even more disheartening, the volume of junk mail containing malicious links is also rising as Spammers see excellent opportunities to fleece generous, but also unwary, citizens.

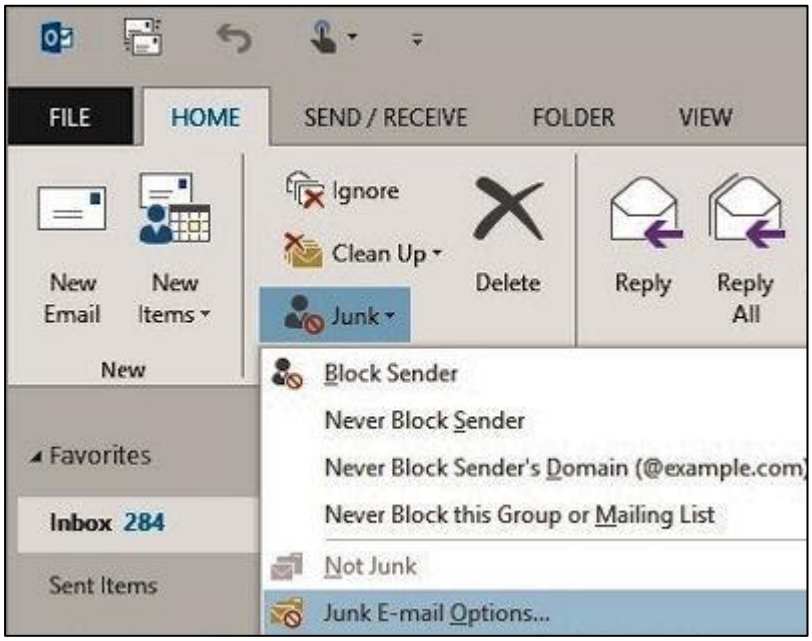
There was a bit of good news in the Kapersky report; the number of phishing emails was down ever so slightly, and malicious files were found in just 2.4 percent of all emails. For the most part, the report confirms what we probably already know, most of the unwelcome mail we receive is annoying but not malevolent. That said, it takes just one email harboring a dangerous attachment or link to wreak havoc on our systems.

The following tips are related to Office 2013 and Outlook.com *(Outlook.com is a free web-based e-mail service provided by Microsoft. It's somewhat like Google's Gmail service but has a twist — a link to your desktop Outlook data. Microsoft has combined Hotmail and Windows Live into one e-mail service and has added support for contacts (including Facebook, Twitter, and LinkedIn) and your calendar. – you can see more HERE)* but also apply directly to Office 2010 and, in general, to earlier versions of Office and other email systems.

Spamming is a sophisticated business. One common technique spammers use to target valid email addresses is to include a *Web beacon* (also known as a Web Bug) inside the message. The process is relatively simple. In a typical email, images download and appear only when you open the message. When the Web server receives the instruction to send picture data, it knows the email address is active. The recipient then get lots more spam. Spammers will often trade or sell their lists of valid addresses, which means you're on the hook for a long time.

Starting with Outlook 2007, Microsoft blocks Web beacons by default. Unless you say otherwise, images in Outlook messages appear as empty boxes with a red **X** inside. If you want to see the images, you have to select the "Click here to download pictures" box at the top of each message. That opens a short list of options such as Download Pictures, Add Sender to Safe Senders list, or Add the Domain {name} to the Safe Senders list. If you pick the latter two options, messages from that particular address will load any included images automatically from then on.

You can also use the Junk tool in Outlook's ribbon to control how Outlook handles mail from specific email addresses or domains. Go to the ribbon's Home tab and click Junk in the Delete group — a list of options will appear, as shown in below.



Selecting Junk E-mail Options opens a toolbox of junk-mail controls. Under the Safe Senders tab, for example, you can quickly add, edit, or remove email addresses and domains. The Add option pops up a simple window for entering trusted email addresses or domains. Email messages from those folks should always get through. You can add an entire domain to the Safe Senders list by clicking Never Block Sender's Domain.

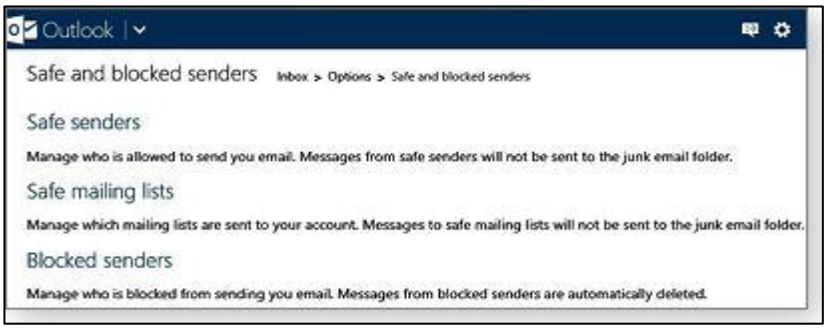
You can also manage the Safe Recipients list via the Junk E-mail Options dialog box. This list works the same way as Safe Senders, but here you add the email addresses that send messages you want to receive.

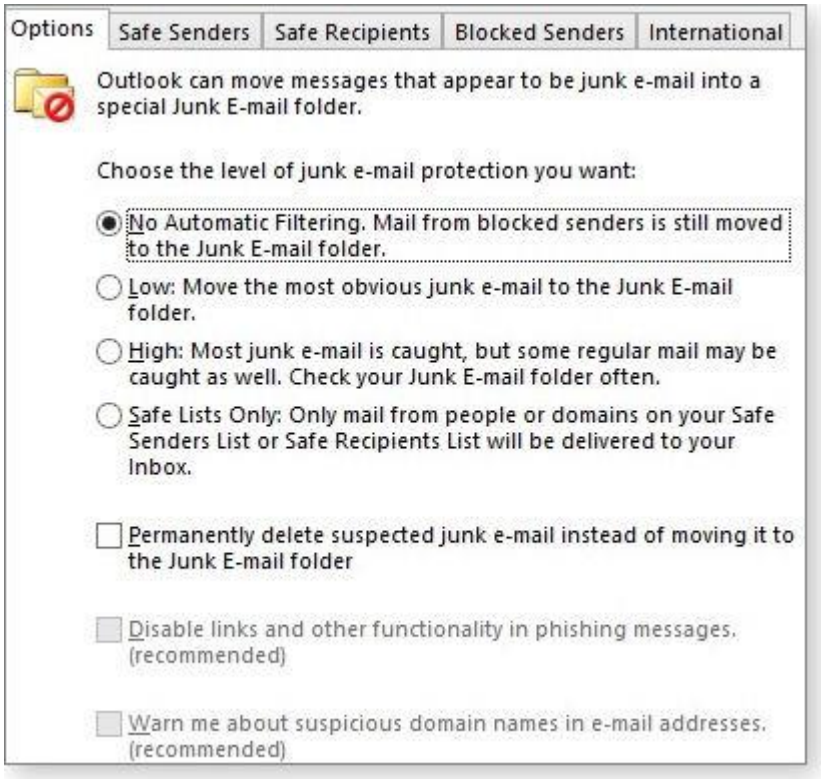
The first checkbox - Also trust e-mail from my Contacts, might be selected by default. The second checkbox - Automatically add people I e-mail to the Safe Senders List, is self-evident.

Unless there's a good possibility you'll email a spammer or someone of questionable character, you can click this checkbox with some confidence of safety.

Microsoft's Web-based email client, Outlook.com, also has tools for adding safe senders and blocking others, but you have far fewer options than in the desktop version of Outlook contained in Office.

To find your Junk Mail lists in Outlook.com, click the gear icon in the top-right corner of Outlook's toolbar and then click More mail settings. In the Options page, choose Safe and blocked senders under the Preventing junk email heading. As the figure at left shows, Outlook.com divides your Safe Senders list into two categories: Safe senders and Safe mailing lists. Use the first one for individuals — friends, colleagues, clients, family, etc.; use the second for mailing lists, newsletters (such as The Radschool Assoc Magazine) and promotions you don't want to end up in the Junk folder.





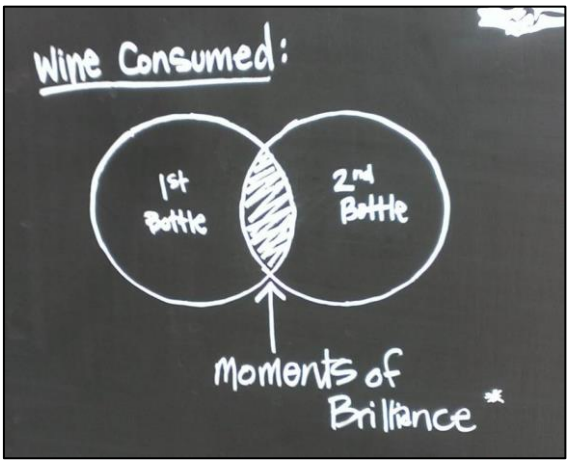
If you use Outlook (the Office version) to handle mail from some other mail service such as Hotmail or Gmail, most spam will never make it to your inbox. There are also numerous third-party, spam-blocking add-ons for Outlook. They're easily found with Google.

For junk mail that does make it through, permanently blocking the sender is easy, select the message and either right-click or click Junk in the ribbon. Either way, you'll get the options shown in the figure at left. Next, select Block Sender. This action adds the person or domain to your Blocked Senders list. Any future mail from a blocked sender should get dumped directly into the Junk E-Mail folder.

In Outlook, you can get tougher on spammers by increasing your level of protection in the Junk Mail settings, as shown in the figure above. You can, for example, have items marked as junk go straight to the trash — no questions asked.

By default, Outlook has the junk-mail protection set to Low — only the most obvious junk mail is automatically moved to the Junk folder (along with messages sent by those in your Blocked

Senders list). Selecting High catches a larger percentage of junk mail but might also grab some messages that aren't junk. Selecting Safe Lists Only dumps into the Junk folder all received mail that isn't from someone listed in Safe Sender or Safe Recipients.
Another check box lets you "Permanently delete suspected junk e-mail instead of moving it to the Junk E-mail folder." However, there's a potential problem with this harder-line approach. Once in a while, messages you'd like to receive will wind up in the junk mail folder. Yes, it's an extra step, but it's safer to review your junk folder before permanently deleting messages.

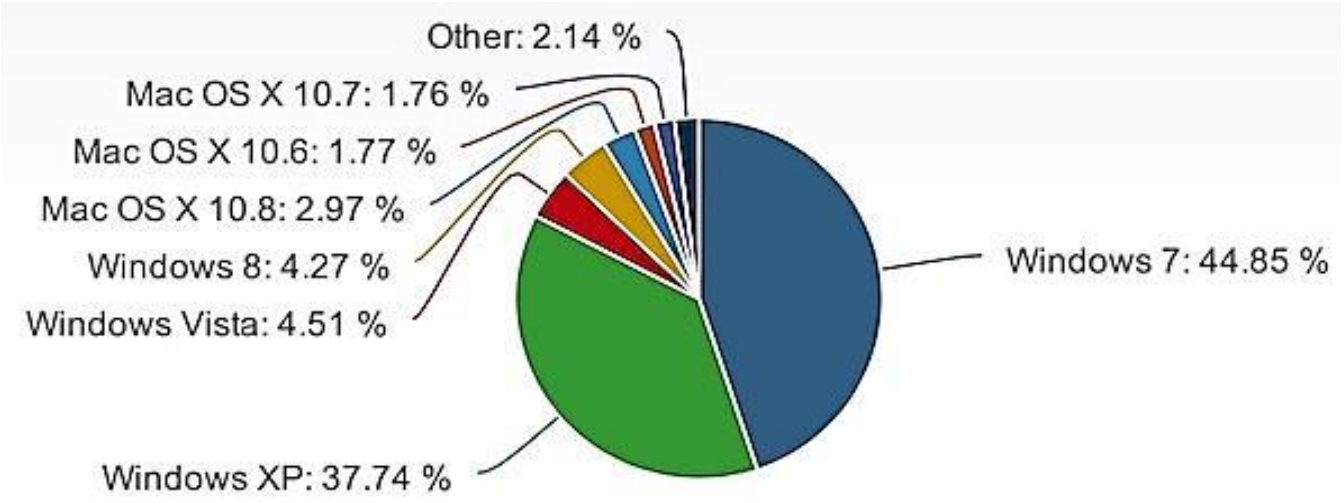


Windows XP

Microsoft's XP operating system is still used on more than a third of the world's PC computers, according to figures from Net Applications. But, is it really still that popular?

XP was released in August of 2001, more than a decade ago. It got a new lease on life when, back in 2007, its successor, Vista, was declared -- at least initially -- a disaster. Recently, XP was shown to retain a robust 37.74 percent of all Windows installations worldwide, (see graph below) down only slightly from 38.31 percent 12 months ago. The continued dependence on XP is potentially a problem for a large segment of users because support for XP will end on April 8, 2014.

Windows XP D-Day will be here before you know it.



You usually don't care what other people are saying, until they start whispering

What really happens when you hit "Like" in Facebook

You've probably seen those pictures posted on Facebook that ask you to "type 'move' into the comments and watch what happens" or "If I get a million likes my dad will get me a car." They seem innocent enough, but they are big business, and you are not doing yourself any favors if you "Like" or "Comment".

The classic example is a colorful picture of a prism with the image from the cover of Pink Floyd's Dark Side of the Moon album in it. It was accompanied by the caption:

"OMG it really works! Step 1: Click on the Picture. Step 2: Hit Like. Step 3: Comment "MOVE" - Then see the Magic!!"

You see in your news feed that your friends have liked and commented on the image, so clearly something amazing must happen when you interact as directed. So you click, you comment, and… nothing happens. Or at least you think nothing happens. But your activity has now spread this image and the page into the news feed of all your friends.

It's called ***"Like Farming"***. Here's how it works.

Someone creates a page and starts posting photos, quotes or other innocent content. You "***Like***" the page and it now shows up regularly on your page. Anytime you click the post, that activity shows up in your friends Facebook page. The more likes the page gets, the more it shows up. The more comments each picture gets, the more power the page gets in the Facebook news feed algorithm. And that makes it more and more visible.

Perhaps the most famous of these "Spams" revolved around a girl called "Mallory". It went like this:

"This is my sister Mallory. She has Down Syndrome (sic) and doesn't think she's beautiful. Please like this photo so I can show her later that she truly is beautiful."

All very nice, but there was no Mallory. The picture was of a young girl named Katie whose mother was horrified that her daughter's image was being used for the scam.

So why would the owners of these pages go to such lengths to scam us into "Liking"? Obviously, because there's money to be made.

When the page gets enough fans (a hundred thousand or more) the owner might start placing ads on the page. Those ads then show up on your page. They could be links to an app, a game, or a service they want you to buy. It could be a "recommendation" for a product where the page owner gets a commission for every purchase made through the link. Or more dishonestly, the page owner could be paid to spread malware by linking out to sites that install viruses on your computer for the purposes of identity theft.

Like any form of Spam, these pages are valuable and can be bought and sold just like any other asset. Online message board, Warriorforum.com listed multiple sites for sale including one page with almost 500,0000 fans of a particular hamburger - price tag - $5000. Another site about “Cuddling: has over a million fans and was listed for sale for $7000.

Facebook say selling pages is specifically against the terms of service and any page(s) that is sold or engages in fraudulent behavior can be removed. But clearly this is a cat and mouse game, with Like Farms popping up on a regular basis.

If you’ve liked something and now regret it, you can unlike it. Go to your profile, choose “more” then “likes” from the drop down menu – then “Unlike.”

A big tip – don’t ***“Like”*** anything…..

How Wireless Gadgets are breaking the Internet

Behind all the dazzling mobile-ready electronics products on display at the recent International Consumer Electronics Show (CES) in Las Vegas was a looming problem - how to make the networks that support all those wireless devices (the iPads, iPhone etc) function robustly and efficiently.

The grand challenge is to overhaul the Internet to better serve an expected flood of 15 billion network-connected devices by 2015, many of them mobile, up from five billion today, according to Intel’s estimates.

The Internet was designed in the 1960s to dispatch data to fixed addresses of static PCs connected to a single network, but today it connects a riot of diverse gadgets that can zip from place to place and connect to many different networks. As the underlying networks have been reworked and added-to to make way for new technologies, some serious inefficiencies and security problems have arisen. "Nobody really expects the network to crash when you add one more device but there is a sense this is more of a creeping problem of complexity."

Over the past year, fundamentally new network designs have taken shape and are being tested at universities around the United States under the National Science Foundation's Future Internet Architectures Project, launched in 2010. One key idea is that networks should be able to obtain data from the nearest location — not seek it from some specific data centre at a fixed address.

If you have a smart phone, an iPod, and a computer and you want to move data from one to the other, that data has to go via the ‘ether’ to a gigantic MSC somewhere in the clouds and then come back via the ‘ether’ to a device that is

only a foot away. All this takes up valuable bandwidth, wastes time and before long will choke up the internet completely. That's crazy.

Scientists are working on a process called "Named Data Networking" (NDN). Under NDN, data packets are assigned addresses that emphasize the information they contain — not just the IP address of where they came from or where they are going. These codes could, among other things, allow easy sharing of data directly between devices. Today data is shared from one device to another via a third party, in the NDN system, you just find the nearest copy of that data and grab it. Conceptually, this is pretty simple, but it is really a revolution."

This data-centric concept would also allow security and privacy settings to be attached directly to the data, with different settings depending on how sensitive the data is, rather than relying on measures such as Virtual Private Networks (VPNs) and firewalls.

One thing is for sure, something is going to have to happen, relatively soon too – otherwise the whole internet will just clog up and we'll be back to sending telegrams instead of emails.

Don't ditch those old Morse skills just yet!!

Whether you believe you can do a thing or not, you are right.

The Blackberry.

It's been a tough couple of years for Research in Motion. The BlackBerry maker still has a faithful following of physical-keyboard loving users, but Apple, Samsung and cheaper smartphone makers from Asia have smashed RIM's market share. Its stock has fallen almost 90% in the last five years and recently posted another weak set of financials. Some say the new BlackBerry 10, (below) the new phone RIM launched on Jan. 30th, could be a make-or-break device.

So what's it like? RIM gave a demo of the phone's software at the Consumer Electronics Show 2013 (CES), unveiling some impressive features. Here are 10 of them, with a video of the demo below.

1. Carriers apparently like it. So far 150 of them from around the world are testing BlackBerry 10 in their labs, which means they'll almost certainly carry the phone. It is expected that 200 carriers will offer BB 10 later this year.
2. The phone is launching with more than 70,000 available apps**,** along with new features to BlackBerry Messenger that RIM will disclose at launch.

3. The phone takes away a physical “home” button — a bit like Nokia’s Lumia phones. It relies on lots of swiping gestures and shortcuts for one-handed use by on-the-go business types.
4. Based on software by QNX, allows users to have two personas on the device – one for work and one for private life, with separate background images and a password that can stop kids from accidentally calling someone’s boss. Users can swap between the two with a single gesture, and decide what content is deemed personal and accessible, or private and professional on the same device.
5. A new feature called BlackBerry Hub. This is a neat amalgamation of all notifications that users access by swiping in an “L” shape, up and to the left. When writing an email and a new one comes in, users can also swipe slightly to “peek” at the content, before continuing with their email. No need to press a button or delete any draft of the email.
6. BlackBerry Hub’s integration with Facebook, Twitter, Foursquare and LinkedIn with potential for other developers to allow their apps to integrate with the Hub too. Users don’t have to go into any of these applications to update their profiles or comment on these networks, but do it all in the Hub.
7. Quick context and aggregation. BlackBerry has created an apparently seamless system that allows you to get relevant information on people in your calendar. Swipe down to see the next appointment, then tap to see previous meetings you’ve had with the person, or what they last said to you in an email, or what a Google search on them brings up, or their LinkedIn profile, all within a couple of windows and without opening a browser.
8. A keyboard that learns. This applies to the touch-screen version of BlackBerry 10, since RIM is bringing out a second BB 10 device with a physical keyboard. The application scans every email or instant message you’ve sent and builds an algorithm to better predict what words you’ll type. Predicted words hover on the “frets” between the key rows, and you select them by flicking up with your thumb (see video below). Swipe down on the keyboard to get punctuation symbols; swipe backwards across the keyboard to erase a word. If you tend to type between the O and P, the keyboard will learn this and shift the touch actuator to lie between the two keys.
9. Language. Start typing the word “je” and the BlackBerry 10 keyboard automatically suggests French words..
10. RIM are yet to unveil a couple of extra features.

Overall, RIM is eagerly promoting BlackBerry 10 and later this year we should know if any of these new features will help RIM stay in the game.

See the video HERE.

Windows 8 startup.

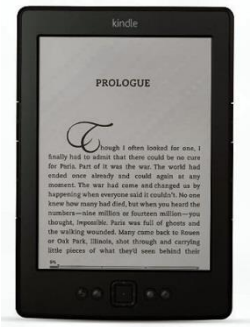
If you’re running a computer with the new Windows 8 software you’re probably wondering how it can start up so quickly when all versions prior to Win 8 took what seemed ages to boot. The answer is in what Microsoft call the “Fast Startup” and it works like this.

That operating system's core never shuts down all the way! When you issue a standard power-down command to Win8, it carries out a ***hybrid shutdown*.** Win8 first closes and terminates everything in the expected way. Next, it copies what's still running in RAM (primarily, the live core of the operating system — the system ***kernel***) onto the hard drive. It then turns off the system hardware. When Win8 starts up after a hybrid shutdown, it performs a ***hybrid boot*.** As soon as the hardware's ready, the core of the OS reloads from the hard drive; Win8 then picks up right from where it left off. Thus, the OS itself is up and ready to go in a flash. You still have to reload your apps and data the normal way though.

That's how it works on most current hardware. However, on some of the newest systems, Win8 can employ an even faster option via a new kind of low-level firmware — Unified Extensible Firmware Interface (UEFI). The UEFI replaces the traditional Basic Input/Output System (BIOS) that's been a part of every PC since the first IBM PC shipped in 1981. Simply put, the BIOS boots and runs the PC until an operating system (Windows, Linux, etc.) wakes up and takes over. The BIOS has worked well for over 30 years, but with new hardware and software, it's showing its limitations. UEFI acts like a BIOS for operating systems that expect to see a BIOS, but it also adds new functions for UEFI-***aware*** OS's, such as Win8.

On a UEFI-equipped PC, Windows 8 can have astonishingly fast startups, especially if the system is also equipped with a solid-state hard drive. How fast? Check out this Microsoft video, which shows a Win8 laptop booting from dead-off to Start Screen in about seven seconds!

Kindle Reader



If you'd rather read your books electronically rather than the traditional paper versions, but don't want to have to buy a Kindle machine, fear not, now you can download all your books directly onto your computer and read them by downloading the FREE app from Amazon. You can get the reader HERE.

Dementia

Dementia projections may be over-pessimistic. The risk of dementia is about 30-40 per cent lower among older men who use computers than among those who do not. This significant difference has been discovered from an eight-year study of more than 5000 Perth men aged 65-85.

A team at the University of Western Australia has been following a group of more than 19,000 men since 1996. "As the world's population ages the number of people experiencing dementia will increase to 50 million by 2025," said Professor Osvaldo Almeida at the UWA-affiliate. the Centre for Health and Ageing.

“1f our findings are correct, the (projected) increase over the next 40 years may not be as dramatic as is currently expect ed.” Prof Aimeida said researchers wondered if computer use could make a difference. “We found that it did, and that there was a significant benefit,” he said.

So!! Let the grand-kids buy their own, keep yours and keep using it..

Legend has it that there is a coffee bar in New York where, in the Ladies Room, there is a very special mirror. If one stands in front of the mirror and tells the truth, one is granted a wish. However, if one tells a lie ---*poof*------- they are instantly swallowed up by the mirror, never to be seen again. Soooooo....
A redhead of questionable looks walks into the ladies room and stands before the mirror and says, "I think I'm the most beautiful woman in the world." *Poof* the mirror swallows her up.
Next a rather large brunette stands before the mirror and says, "I think I'm the sexiest woman alive". *Poof* the mirror swallows her.
Then, an absolutely gorgeous blond comes in and stands before the mirror and says, "I think...". *Poof*

Skype.

Few internet advances have compressed space between people as thoroughly as Skype. The internet telephony service began in 2003 and is now used by more than 300 million people. The plan was to spark new ways of behaviour when Swedish software designer Niklas Zennstrom met with Dane Janus Friis in Copenhagen. Both had experience in online music exchanges and wanted to try their hand at online telephony.

As with their prior project, Kazaa, they relied on peer-to-peer technology. Using a vast number of private computers is not just cheaper than setting up a central server as a hub but also makes it very difficult for attackers to knock the system out. Friis (right) mentioned the project, calling it Skyper – a combination of ‘sky’ and ‘peer-to-peer’ – to a Danish newspaper at the end of 2002. “We think it has the potential to get as big as Kazaa,” he said. Skyper became Skype and it certainly did get as big as Kazaa, which later went out of existence. But it had some delicate first steps. The site was registered on April 23, 2003, with Estonian Ahti Heinla handling most of the programming.

Things really got going on August 29 that year with the release of the first Skype software. “When I tried to raise money for Skype, it took

almost a year," Zennstrom (left) said, looking back at the rough first year. Internet telephony existed before Skype. US company Net2Phone was founded in 1996. In 2001, there was Vonage. But most of those relied upon SIP (Session Initiation Protocol). Skype came up with its own technology, "because SIP couldn't deliver what we wanted," said Friis in a 2003 interview.

That step allowed Skype to offer better speech quality with a simple set-up. Skype communications whether text, audio or video, are encrypted, with a method the company keeps secret. That initially made the service popular among those interested in privacy, though Skype has since agreed to release data in criminal investigations.

Skype's software was downloaded 60,000 times in its first weeks in 2003. At times, its server was overwhelmed by demand. Its success also changed the telecommunications industry. "I knew it was over when I downloaded Skype," said Michael Powell, former head of the US Federal Communications Commission, in 2004. "The world will now change inevitably." By October 2004, there were more than one million Skype users.

However, there was resistance from established telecommunications companies, which tried to block Skype signals, calling into question the equal treatment of different kinds of data online. Legal action was required to clear the logjam but the image of Skype as a bunch of net rebels didn't last long.

Skype was purchased by eBay in 2005 for about $US3.1 billion ($A3.03 billion), though it did not quite fulfil expectations and was sold on in 2009 to the Silver Lake investment group. But interest remained and Microsoft eventually purchased Skype for $US8.5 billion ($A8.30 billion). The company recorded another milestone at the start of April, logging more than two billion minutes of chats and telephone calls a day. It claims 300 million users are active at least once a month. At peak times, 50 million users are simultaneously linked, with duration of use up 58 per cent in the first quarter over the same period in 2012.

I was having trouble with my computer, so I called Eric, the 11 year old kid next door, whose bedroom looks like Mission Control and asked him to come over. Eric clicked a couple of buttons and solved the problem. As he was walking away, I called after him, 'So, what was wrong? He replied, 'It was an ID ten T error.' I didn't want to appear stupid, but nonetheless inquired, 'An, ID ten T error? What's that? In case I need to fix it again. 'Eric grinned.... 'Haven't you ever heard of an ID ten T error before? 'No,' I replied. 'Write it down,' he said, 'and I think you'll figure it out.' So I wrote down: ID10T

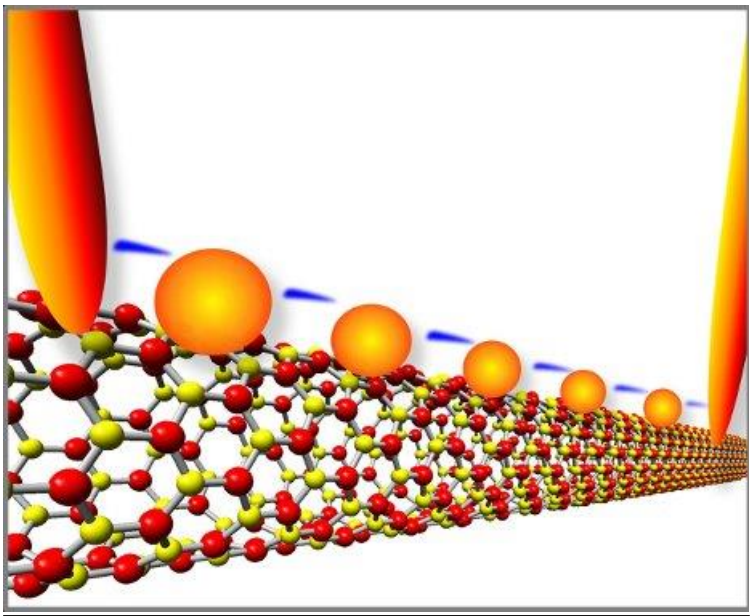
I used to like Eric, the little bastard.

Beyond Silicon: Transistors without Semiconductors

For decades, electronic devices have been getting smaller, and smaller, and smaller. It's now possible—even routine—to place millions of transistors on a single silicon chip. But transistors based on semiconductors can only get so small. "At the rate the current technology is progressing, in 10 or 20 years, they won't be able to get any smaller," said physicist Yoke Khin Yap of Michigan Technological University. "Also, semiconductors have another disadvantage: they waste a lot of energy in the form of heat."

Scientists have experimented with different materials and designs for transistors to address these issues, always using semiconductors like silicon. Back in 2007, Yap wanted to try something different that might open the door to a new age of electronics. "The idea was to make a transistor using a nanoscale insulator with nanoscale metals on top," he said. "In principle, you could get a piece of plastic and spread a handful of metal powders on top to make the devices, if you do it right. But we were trying to create it in nanoscale, so we chose a nanoscale insulator, boron nitride nanotubes, or BNNTs for the substrate."

Yap's team had figured out how to make virtual carpets of BNNTs, which happen to be insulators and thus highly resistant to electrical charge. Using lasers, the team then placed quantum dots (QDs) of gold as small as three nanometers across on the tops of the BNNTs, forming QDs-BNNTs. BNNTs are the perfect substrates for these quantum dots due to their small, controllable, and uniform diameters, as well as their insulating nature. BNNTs confine the size of the dots that can be deposited.



Electrons flash across a series of gold quantum dots on boron nitride nanotubes. Michigan Tech scientists made the quantum-tunnelling device, which acts like a transistor at room temperature, without using semiconducting materials.

They fired up electrodes on both ends of the QDs-BNNTs at room temperature, and something interesting happened. Electrons jumped very precisely from gold dot to gold dot, a phenomenon known as quantum tunnelling. "Imagine that the nanotubes are a river, with an electrode on each bank. Now imagine some very tiny stepping stones across the river," said Yap. "The electrons hopped between the gold stepping stones. The stones are so small, you can only get one electron on the stone at a time. Every electron is passing the same way, so the device is always stable."

Yap's team had made a transistor without a semiconductor. When sufficient voltage was applied, it switched to a conducting state. When the voltage was low or turned off, it reverted to its natural state as an insulator.

O

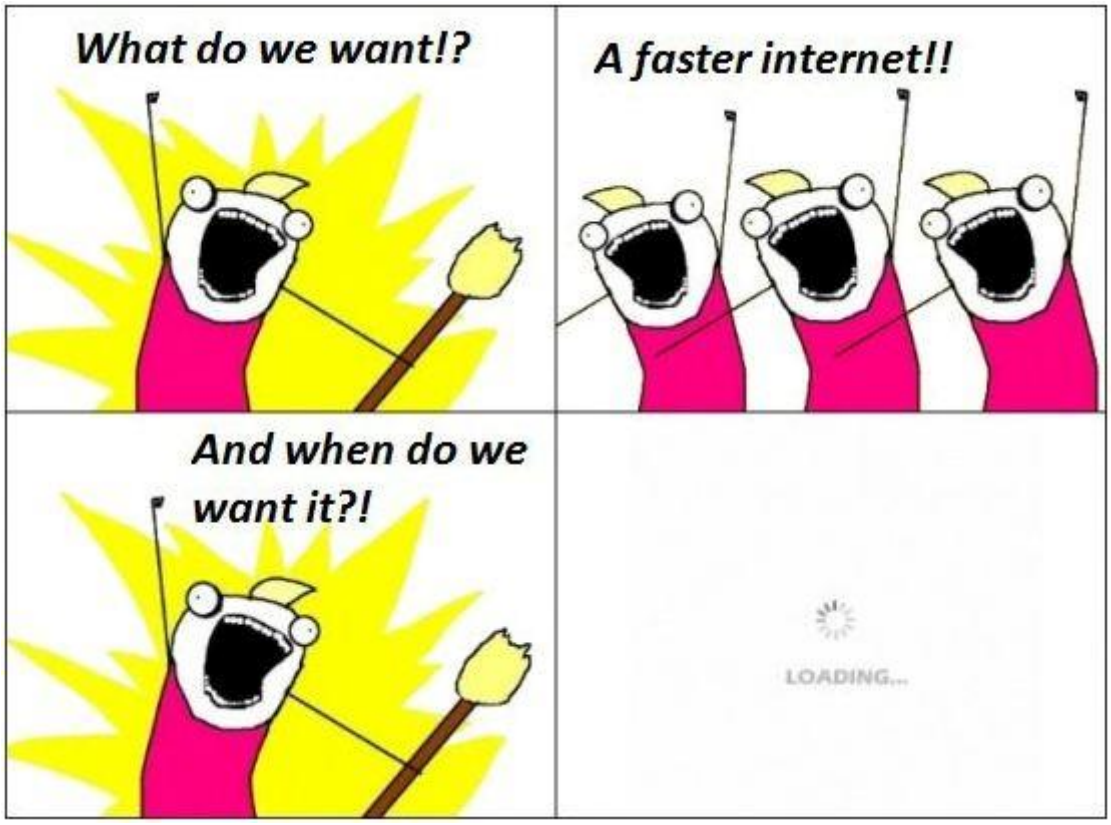
Furthermore, there was no “leakage”: no electrons from the gold dots escaped into the insulating BNNTs, thus keeping the tunnelling channel cool. In contrast, silicon is subject to leakage, which wastes energy in electronic devices and generates a lot of heat.

Other people have made transistors that exploit quantum tunnelling, however, those tunnelling devices have only worked in conditions that would discourage the typical cell-phone user, they only operate at liquid-helium temperatures.

The secret to Yap’s gold-and-nanotube device is its submicroscopic size: one micron long and about 20 nanometers wide. The gold islands have to be on the order of nanometers across to control the electrons at room temperature, because if they are too big, too many electrons can flow. In this case, smaller is truly better: Working with nanotubes and quantum dots gets you to the scale you want for electronic devices.

Theoretically, these tunnelling channels can be miniaturized into virtually zero dimension when the distance between electrodes is reduced to a small fraction of a micron.

There is going to be some amazing stuff out there in 20 years, that’s for sure.




Alcohol!
Because No great
Story started with
Someone eating
a Salad.

This page left blank.