Computers and Stuff.

Sam Houliston.

Can you get a virus using Apple computers?

This has been the topic of discussion for a long time and there has even been talk about suing Apple for false claims. Imagine this scenario, your grandparents want to buy a computer and you (and Apple) tell them that Apple is completely safe. Then they get one phishing email and their life-savings are gone! That could be very interesting!

The story about there being no viruses that attack Apple is one of those rumours spread around the Internet by a bunch of fan boys. It is NOT true. If you don't believe that, go to any major website that lists details of viruses and look for one affecting Apple MACs. You'll find enough there. Go to the NIST website and look up vulnerabilities. If Apple users have not been patching their machines, they could be in for a big surprise. Apple does release security patches.

Apple products are generally more secure than Windows though much of this has been attributed to hackers not wanting to bother with Apple, as a while ago Apple ran second and a long way back in numbers in use compared to PC. There was a Russian group that specialized in Apple mischief but they were all arrested a few years ago. But Apple is catching up and the hackers are starting to notice.

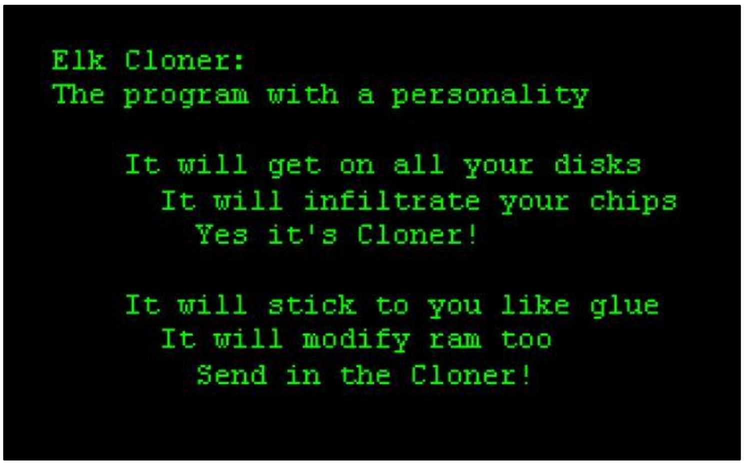
HERE is just one Apple Virus, You will find a lot more.

Don't be blinkered, always keep your Apple device up to date with the latest patch otherwise you could be in for a big bad shock.

It says I should regularly back up my hard drive? How do I put in reverse?

History of Viruses.

The term “computer virus" was formally defined by Fred Cohen in 1983 while he performed academic experiments on a Digital Equipment Corporation VAX system. Viruses are classified as being one of two types: “Research” or “In the Wild." A Research virus is one that has been written for research or study purposes and has received almost no distribution to the public. On the other hand, viruses which have been seen with any regularity are termed “In the Wild." The first Research computer viruses were developed in the early 1980s and the first viruses found In the Wild were Apple II viruses, such as Elk Cloner, which was reported in 1981.



```
Elk Cloner:
The program with a personality

    It will get on all your disks
      It will infiltrate your chips
        Yes it's Cloner!

    It will stick to you like glue
      It will modify ram too
        Send in the Cloner!
```

Viruses have been found on the following platforms:

- Apple II
- IBM PC
- Macintosh
- Atari
- Amiga

The overwhelming number of virus strains were initially IBM PC viruses. Viruses “evolved" over the years due to efforts by their authors to make the code more difficult to detect, disassemble, and eradicate. This evolution has been especially apparent in the IBM PC viruses since there were more distinct viruses known for the DOS operating system than any other.

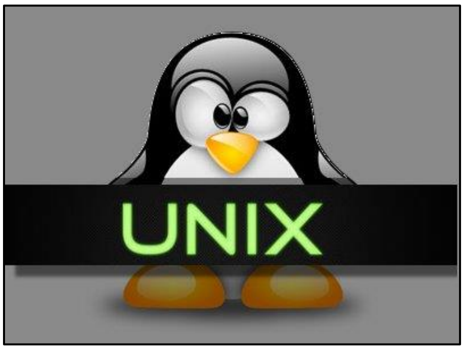
The first IBM-PC virus appeared in 1986. This was the *Brain* virus. *Brain* was a boot sector virus and remained resident. In 1987, *Brain* was followed by *Alameda* (*Yale*), *Cascade*, *Jerusalem*, *Lehigh*, and *Miami* (*South African Friday the 13th*). These viruses expanded the target executables to include COM and EXE files. *Cascade* was encrypted to deter disassembly and detection. Variable encryption appeared in 1989 with the *1260* virus. Stealth viruses, which employ various techniques to avoid detection, also first appeared in 1989, such as *Zero Bug*, *Dark Avenger* and *Frodo* (*4096* or *4K*). In 1990, self-modifying viruses, such as *Whale* were introduced. The year 1991 brought the *GP1* virus, which is “network-sensitive" and attempted to steal Novell NetWare passwords. Since their inception, viruses have become increasingly complex.

Examples from the PC family of viruses indicate that the most commonly detected viruses vary according to continent, but *Stoned*, *Brain*, *Cascade*, and members of the *Jerusalem* family, have spread widely and continue to appear. This implies that highly survivable viruses tend to be benign, replicate many times before activation, or are somewhat innovative, utilizing some technique never used before in a virus.

Personal computer viruses exploit the lack of effective access controls in these systems. The viruses modify files and even the operating system itself. These are “legal" actions within the context of the operating system. While more stringent controls are in place on multi-tasking, multi-user operating systems, configuration errors, and security holes (security bugs) make viruses on these systems more than theoretically possible.

This leads to the following initial conclusions:

- Viruses exploit weaknesses in operating system controls and human patterns of system use/misuse.
- Destructive viruses are more likely to be eradicated.
- An innovative virus may have a larger initial window to propagate before it is discovered and the “average" anti-viral product is modified to detect or eradicate it.



It has been suggested that viruses for multi-user systems are too difficult to write. However, Fred Cohen required only 8 hours of expert work' to write a virus that could penetrate a UNIX system. The most complex PC viruses required a great deal more effort.

Yet, if we reject the hypothesis that viruses do not exist on multi-user systems because they are too difficult to write, what reasons could exist? Perhaps the explosion of PC viruses (as opposed to other personal computer systems) can provide a clue. The population of PCs is by far the largest. Additionally, personal computer users exchanged disks frequently. Exchanging disks is not required if the systems are all connected to a network. In this case large numbers of systems may be infected through the use of shared network resources.

One of the primary reasons that viruses have not been observed on multi-user systems is that administrators of these systems are more likely to exchange source code rather than executables. They tend to be more protective of copyrighted materials, so they exchange locally developed or public domain software. It is more convenient to exchange source code, since differences in hardware architecture may preclude exchanging executables.

The advent of remote disk protocols, such as NFS (Network File System) and RFS (Remote File System) have resulted in the creation of many small populations of multi-user systems which freely exchange executables. Even so, there is little exchange of executables between different “clusters" of systems.

Current protection against Viruses.

Although many anti-virus tools and products are now available, personal and administrative practices and institutional policies, particularly with regard to shared or external software usage, should form the first line of defence against the threat of virus attack closely followed by keeping your software, particularly operating system software, up to date. Users should also consider the variety of anti-virus products currently available.

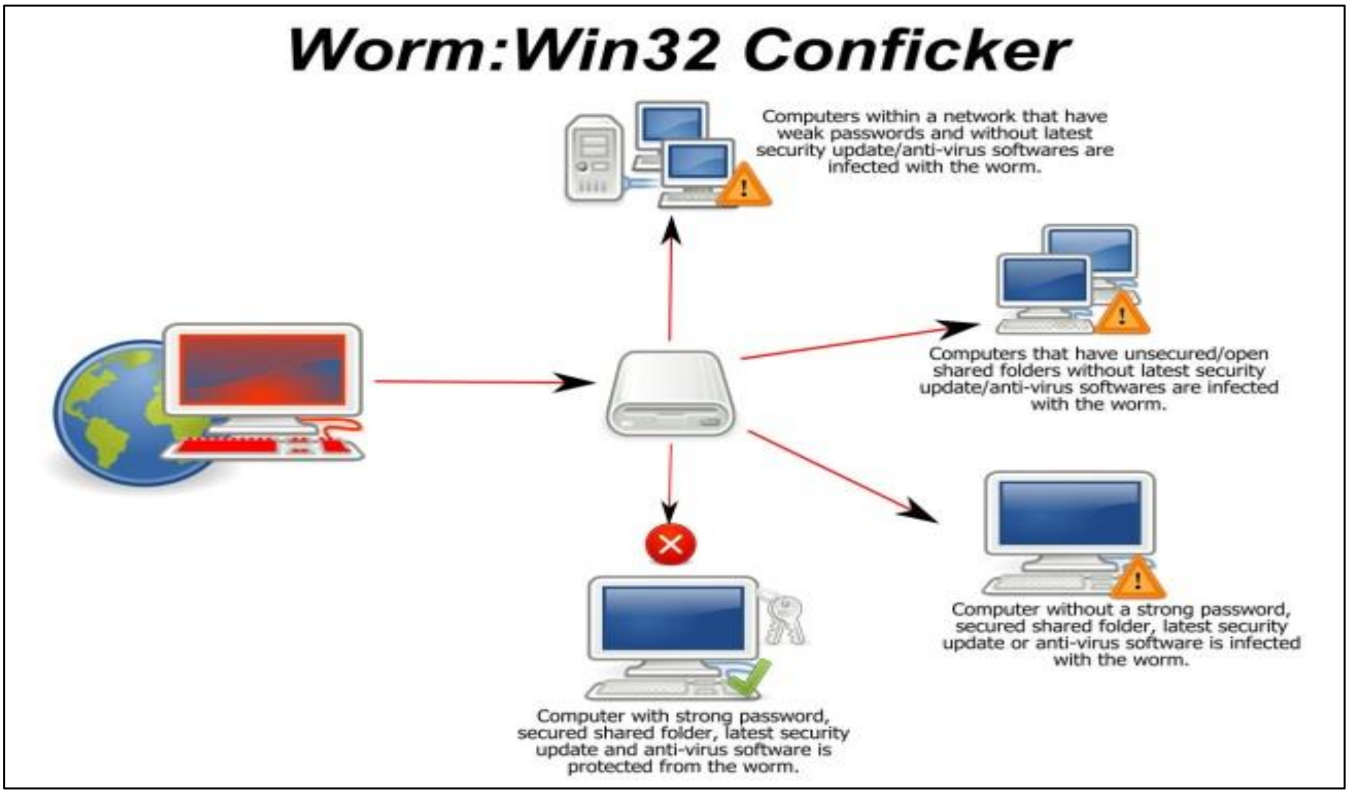
There are three classes of anti-virus products: Detection tools, Identification tools, and Removal tools. Scanners are an example of both detection and identification tools. Vulnerability monitors and modification detection programs are both examples of detection tools. Disinfectors are examples of a removal tools.

Scanners and disinfectors, the most popular classes of anti-virus software, rely on a great deal of *a priori* knowledge about the viral code. Scanners search for “signature strings" or use algorithmic detection methods to identify known viruses. Disinfectors rely on substantial information regarding the size of a virus and the type of modifications to restore the infected file's contents.

Vulnerability monitors, which attempt to prevent modification or access to particularly sensitive parts of the system, may block a virus from hooking sensitive interrupts. This requires a lot of information about “normal" system use, since personal computer viruses do not actually circumvent any security features. This type of software also requires decisions from the user.

Modification detection is a very general method, and requires no information about the virus to detect its presence. Modification detection programs, which are usually checksum based, are used to detect virus infection or Trojan horses. This process begins with the creation of a baseline, where checksums for clean executables are computed and saved. Each following iteration consists of checksum computation and comparison with the stored value. It should be noted that simple checksums are easy to defeat; cyclical redundancy checks (CRC) are better, but can still be defeated; cryptographic checksums provide the highest level of security.

Worms.


Worm:Win32 Conficker
Computers within a network that have weak passwords and without latest security update/anti-virus softwares are infected with the worm.
Computers that have unsecured/open shared folders without latest security update/anti-virus softwares are infected with the worm.
Computer without a strong password, secured shared folder, latest security update or anti-virus software is infected with the worm.
Computer with strong password, secured shared folder, latest security update and anti-virus software is protected from the worm.

The following are necessary characteristics of a worm:

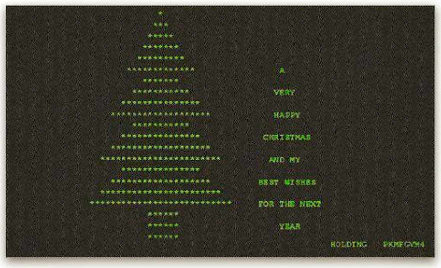
- replication
- self-contained; does not require a host
- activated by creating process (needs a multi-tasking system)
- for network worms, replication occurs across communication links

A worm is not a Trojan horse, it is a program designed to replicate and may perform any variety of additional tasks as well. The first network worms were intended to perform useful network management functions. They took advantage of system properties to perform useful action, however, a malicious worm takes advantage of the same system properties. The facilities that allow such programs to replicate do not always discriminate between malicious and good code.

History of Worms.

Worms were first used as a legitimate mechanism for performing tasks in a distributed environment. Network worms were considered promising for the performance of network management tasks in a series of experiments at the Xerox Palo Alto Research Center in 1982. The key problem noted was “worm management;'' controlling the number of copies executing at a single time. This would be experienced later by authors of malicious worms.

Worms were first noticed as a potential computer security threat when the *Christmas Tree Exec* attacked IBM mainframes in December 1987. It brought down both the world-wide IBM network and BITNET. The *Christmas Tree Exec* wasn't a true worm. It was a trojan horse with a replicating mechanism. A user would receive an e-mail Christmas card that included executable (REXX) code which if executed the program claimed to draw a Christmas Tree on the display. That much was true, but it also sent a copy to everyone on the user's address lists.



```
A
VERY
HAPPY
CHRISTMAS
AND MY
BEST WISHES
FOR THE NEXT
YEAR
                HOLDING   PKMFGVM4
```

The *Internet Worm* was a true worm. It was released on November 2, 1988. It attacked Sun and DEC UNIX systems attached to the Internet (it included two sets of binaries, one for each system). It utilized the TCP/IP protocols, common application layer protocols, operating system bugs, and a variety of system administration flaws to propagate. Various problems with worm management resulted in extremely poor system performance and a denial of network service.

The *Father Christmas* worm was also a true worm. It was first released onto the worldwide DECnet Internet in December of 1988. This worm attacked VAX/VMS systems on SPAN and HEPNET. It utilized the DECnet protocols and a variety of system administration flaws to propagate. The worm exploited TASK0, which allows outsiders to perform tasks on the system. This worm added an additional feature; it reported successful system penetration to a specific site.

This worm made no attempt at secrecy; it was not encrypted and sent mail to every user on the system. About a month later another worm, apparently a variant of *Father Christmas*, was released on a private network. This variant searched for accounts with “industry standard" or “easily guessed" passwords.

The history of worms displays the same increasing complexity found in the development of PC viruses. The *Christmas Tree Exec* wasn't a true worm. It was a Trojan horse with a replicating mechanism. The *Internet Worm* was a true worm; it exploited both operating system flaws and common system management problems. The DECnet worms attacked system management problems, and reported information about successful system penetration to a central site.

Several conclusions can be drawn from this information:

- worms exploit flaws (i.e, bugs) in the operating system or inadequate system management to replicate.
- release of a worm usually results in brief but spectacular outbreaks, shutting down entire networks.

A Jewish mother gives her son a blue shirt and a brown shirt for his birthday. On the next visit, he wears the brown one. The mother says, "What's the matter already? Didn't you like the blue one?"

Yes Script, No Script.

Bob Webster.

It really irritates me when I'm reading something on the internet and a flyover window comes across and blocks my view. I also am not a fan of animated sliders for ads and menus. They can be good as an integral part of a site however, it's really dumb in a menu or advertisement when text scrolls away while you're reading it, or if you have to wait on it to scroll away when you're ready for the next page.

Companies use these things a lot because:

(a) they're easy to implement on a web site,
(b) they look cool in a presentation to management, particularly when management doesn't use the site, and
(c) some companies don't care what users think because their customers are not their users. Their customers are companies to whom they sell their users' data.

I started to go on a rampage and destroy all the web sites I found offensive. Well, offensive in design, not content. I do have a limited lifespan so I opted to leave the internet intact and change my web browsers instead.

With Firefox, I use Yesscript (you can get it HERE). Yesscript gives you a button you can click to disable Javascript on a site. Javascript is the source of most of the over-animated slideshows and flyover windows. Whenever one of those things intrudes onto my screen, I zap Javascript for the site, and it remembers not to load Javascript on that site any more.

Javascript is necessary on some sites such as e-commerce sites, financial sites, and chess.com, so it's useful not to disable it in the browser entirely. In fact, a few months ago Firefox removed that option.

I also use Ghostery and Adblock Plus on both Firefox and Chrome. These trim down the web traffic considerably and keep the display, for the most part, static. A significant side effect is that web pages load a lot faster when they don't have to load all the extra trash.

You can block the majority of the garbage -- ads, marketing scripts, etc., using the Firefox or Chrome extensions Adblock Plus and Ghostery. I don't use Internet Explorer or Safari, but there is probably something similar for them.

Adblock Plus is particularly useful. I hear people complain about ads on Facebook, for example, but I've never seen one. Slashdot offers me a checkbox to stop ads, as some kind of valued user, but I don't see any ads to begin with.

One of life's greatest mysteries is how the boy who wasn't good enough to marry your daughter can be the father of the smartest grandchild in the world.

E-Mail Good Sense!

By now, I suspect everyone is familiar with snopes.com and/or truthorfiction.com for determining whether information received via email is just that - true/false or fact/fiction. Both are excellent sites. Sometimes it is a good idea to check out something on one of the two sites before forwarding to check validity!

1. Any time you see an email that says "forward this on to '10' (or however many) of your friends", "sign this petition", or "you'll get bad luck" or "you'll get good luck" or "you'll see something funny on your screen after you send it" or whatever --- it almost always has an email tracker program attached that tracks the cookies and emails of those folks you forward to. The host sender is getting a copy each time it gets forwarded and then is able to get lists of 'active' email addresses to use in SPAM emails or sell to other Spammers. Even when you get emails that demand you send the email on if you're not ashamed of God/Jesus

that is email tracking and they are playing on our conscience. These people don't care how they get your email addresses - just as long as they get them. Also, emails that talk about a missing child or a child with an incurable disease "how would you feel if that was your child" is nearly always email tracking. Ignore them and don't participate!

2. Almost all emails that ask you to add your name and forward on to others are similar to that mass letter years ago that asked people to send business cards to the little kid in Florida who wanted to break the Guinness Book of Records for the most cards. All it was, and all any of this type of email is, is a way to get names and 'cookie' tracking information for telemarketers and Spammers -- to validate active email accounts for their own **profitable** purposes.

You can do your Friends and Family members a great favour by sending this information to them. You will be providing a service to your friends. And you will be rewarded by not getting thousands of spam emails in the future!

You can do yourself a favour and **STOP** adding your name(s) to those types of listing regardless how inviting they might sound or make you feel guilty if you don't! It's all about getting email addresses and nothing more. You may think you are supporting a great cause, but you are NOT!

Instead, you will be getting tons of junk mail later and very possibly a virus attached! Plus, you will be we are helping the Spammers get rich! Don't make it easy for them!

And another important point is to delete all previous names from your emails before forwarding!!! Send emails to your entire address list BC (Blind Copy) then everyone after you doesn't get your friend's email address. Search the help if your email program doesn't list this.

Telemarketing.

Most of us hate receiving telemarketing calls or junk mail, either in the letter box or the email in-box and when someone comes out with a "fix" we're prepared to give it a go – but are these "fixes" any good??

You have probably read somewhere that the best way to stop receiving telemarketing calls is to use these three little words!! - 'Hold On, Please...' You would have read that "Saying this, while putting down your phone and walking off (instead of hanging-up immediately) would make each telemarketing call so much more time-consuming that sales would grind to a halt. Then when you eventually hear the phone company's 'beep-beep-beep' tone, you know it's time to go back and hang up your handset, which has efficiently completed its task."

And,

“Do you ever get those annoying phone calls with no one on the other end? This is a telemarketing technique where a machine makes phone calls and records the time of day when a person answers the phone. This technique is used to determine the best time of day for a 'real' sales person to call back and get someone at home. What you can do after answering, if you notice there is no one there, is to immediately start hitting your # button on the phone, 6 or 7 times as quickly as possible. This confuses the machine that dialled the call and it kicks your number out of their system.”

And,

“When you get ads enclosed with your phone or electricity bill or some other bill, return these ads with your payment. Let the sending companies throw their own junk mail away. When you get those 'pre-approved' letters in the mail for everything from credit cards or similar type junk, do not throw away the return envelope. Most of these come with postage-paid return envelopes, right? It costs them more than the regular postage, 'IF' and when they receive them back. It costs them nothing if you throw them away! And why not get rid of some of your other junk mail as well and put it in these cool little postage-paid return envelopes. Send an ad for your local chimney cleaner to American Express. Send a pizza coupon to Citibank. If you didn't get anything else that day, then just send them their blank application back!

If you want to remain anonymous, just make sure your name isn't on anything you send them. You can even send the envelope back empty if you want to just to keep them guessing! The banks and credit card companies are currently getting a lot of their own junk back in the mail, but folks, we need to OVERWHELM them. Let's let them know what it's like to get lots of junk mail, and best of all they're paying for it...Twice!”

If enough people follow these tips, it will work I have been doing this for years, and I get very little junk mail anymore.”

Don’t believe a word of it, it’s all rubbish!!!!

If you want to stop receiving annoying telemarketing calls the only way is to put your name and phone numbers (land-line and mobile) with the Do Not Call Register administered by the Australian Communications and Media Authority (ACMA). You can do that HERE – and it’s free.

If you want to stop receiving advertisements tucked away in legitimate mail, (via the Post), you can register with the Association for Data-driven Marketing and Advertising Association (ADMA). You can do that for free HERE. Registering with ADMA will not stop all marketing, but it will stop a lot.

It will **not stop** or reduce the amount of addressed mail you receive from:

- Companies of which you are a current customer
- Companies that are not members of ADMA
- Businesses that market themselves to your business
- The delivery of unaddressed mail, including brochures, letterbox drops and flyers.

Intellectuals solve problems; geniuses prevent them.

Underused tools hiding in Windows 7 and Windows 8.

Windows Secrets
Everything Microsoft forgot to mention.

Back in Windows' younger and simpler days, its coders hid small programs and features, called Easter Eggs, in the OS for others to find.

Microsoft declared a ban on Easter eggs as part of its 2005 Trustworthy Computing policy but there are still some relatively hidden features in Win7/8 that users find helpful. In Oct. 2005, Microsoft developer Larry Osterman gave various reasons for the ban on unofficial code in the company's products but security was likely the main concern. The undocumented code in an Easter egg might be a benign bit of fun, but it might also allow malware into Windows or another MS application.

Easter eggs, and any other unofficial code, were finally eliminated with Windows 7. Even so, there are still some stealth productivity tricks buried in Win7 and Win8.1 which are activated by various methods such as digging deep into menus or cutting and pasting random phrases. Here are some that are hiding in plain sight.

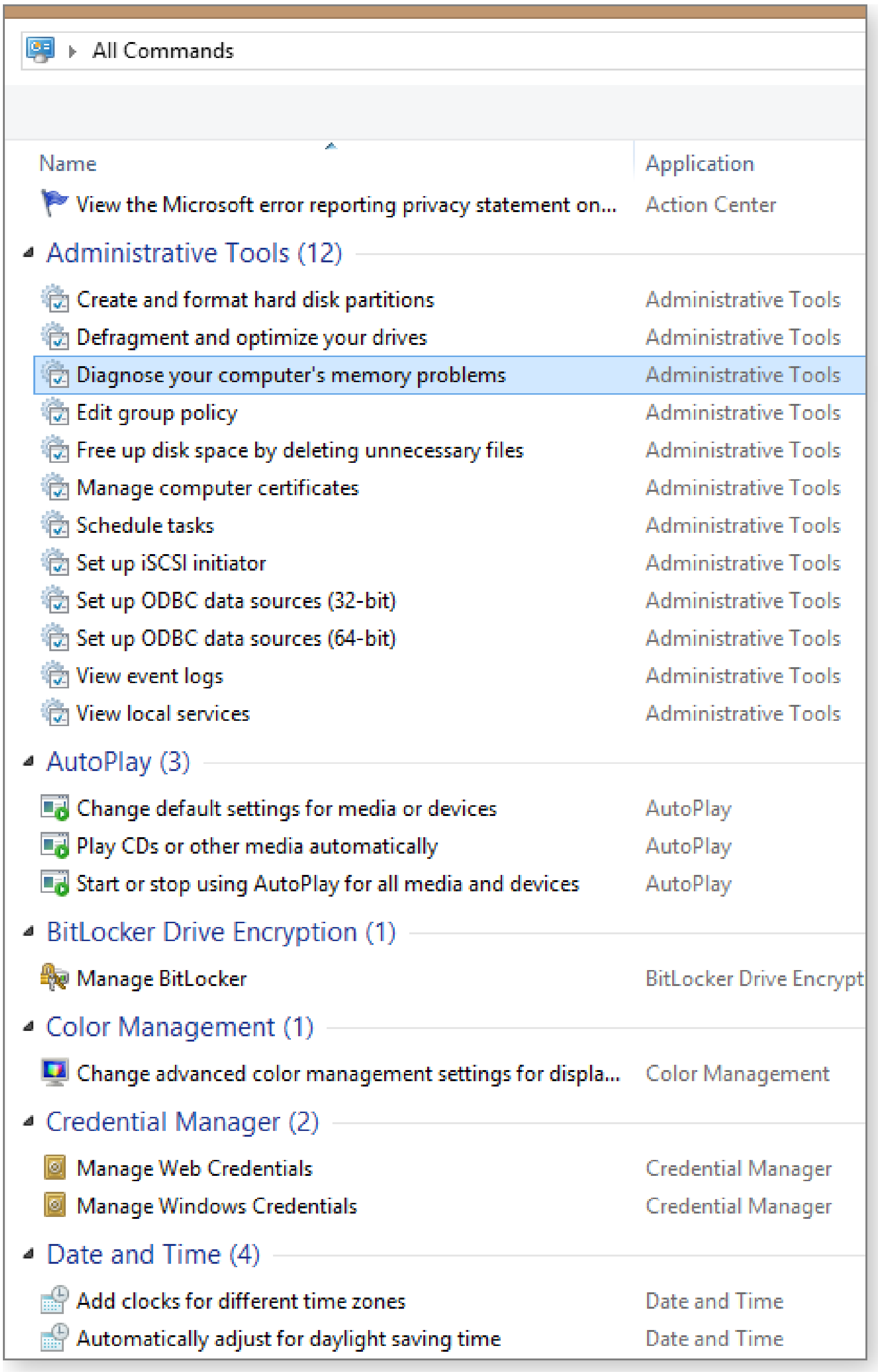
Command Central: Windows functions in one place.

How did an essentially undocumented trick, designed for IT administrators and commonly called GodMode, go viral on the Internet? Certainly the all-powerful connotation of the name aroused interest but it's this function's one-stop list of Windows tools that wins over most users.

Whatever you wish to call this function, it conveniently consolidates into one folder a veritable switchboard of configurable Windows options and commands. The 256 items (sorted into 45 categories) are typically buried under layers of Control Panel menus or in right-click submenus or otherwise submerged in the vast number of admin tools in Windows.

To create this folder, take the following steps:

- Right-click a free spot on the desktop and select New/Folder.
- Give the new folder any name you wish, as long as it's followed by a period and the following string of characters: **{ED7BA470-8E54-465E-825C-99712043E01C}** (Example: **All Commands.{ED7BA470-8E54-465E-825C-99712043E01C}**
- Double-click to open the folder, and you will see more than 250 functions, as below.



All Commands

Name	Application
View the Microsoft error reporting privacy statement on...	Action Center
Administrative Tools (12)	
Create and format hard disk partitions	Administrative Tools
Defragment and optimize your drives	Administrative Tools
Diagnose your computer's memory problems	Administrative Tools
Edit group policy	Administrative Tools
Free up disk space by deleting unnecessary files	Administrative Tools
Manage computer certificates	Administrative Tools
Schedule tasks	Administrative Tools
Set up iSCSI initiator	Administrative Tools
Set up ODBC data sources (32-bit)	Administrative Tools
Set up ODBC data sources (64-bit)	Administrative Tools
View event logs	Administrative Tools
View local services	Administrative Tools
AutoPlay (3)	
Change default settings for media or devices	AutoPlay
Play CDs or other media automatically	AutoPlay
Start or stop using AutoPlay for all media and devices	AutoPlay
BitLocker Drive Encryption (1)	
Manage BitLocker	BitLocker Drive Encrypt
Color Management (1)	
Change advanced color management settings for displa...	Color Management
Credential Manager (2)	
Manage Web Credentials	Credential Manager
Manage Windows Credentials	Credential Manager
Date and Time (4)	
Add clocks for different time zones	Date and Time
Automatically adjust for daylight saving time	Date and Time

Of course, any one of these functions can be called up from the Windows search bar but if you don't recall a specific function's name, good luck with that route. Your new all-commands folder should make a needed tool quick to find and easy to launch.

Pin folders and icons to the Win8 Start screen.

As with many long-time Windows users still tied to a keyboard and mouse, I rarely venture into Windows 8's Modern User Interface. But the Win8 Start screen can be a good place to organize

K

folders and other frequently used sites and apps. Sure, with Win8.1 you can now pin native Win8 apps to the Desktop taskbar, but that's extremely limited real estate.

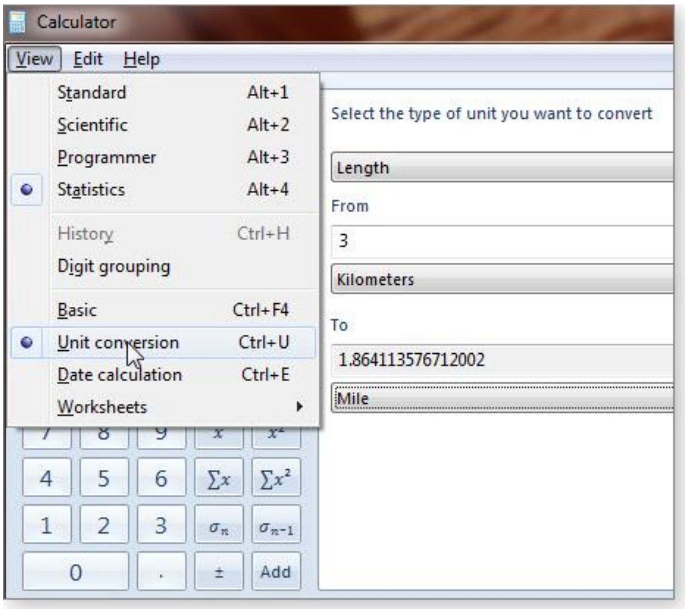
So the **Pin to Start** function, available by right-clicking any folder or application icon, can be particularly handy. As an example, right-click the aforementioned All Commands (GodMode) folder you created on the Win8 Desktop and click Pin to Start. You'll now find on the Start screen a new movable tile labeled All Commands. Clicking the tile instantly returns you to the Desktop, with the All Commands folder open, no need to clutter up your Desktop or taskbar.

A related trick is one that's often overlooked. You easily create shortcuts to frequently visited websites. For example, you can easily create a shortcut to the Radschool web site, just right-click anywhere on the desktop, select New/Shortcut, and then type www.radschool.org.au into the location box. Click Next and give the shortcut a name. Click Finish when you're done.

Keep in mind that the shortcut can live only on the desktop. Unlike apps, shortcuts for websites can't be pinned to the Start screen or the taskbar (although files, folders, and website shortcuts can be pinned to associated apps that are pinned to the taskbar).

Calculator: Do much more than simple arithmetic

Another overlooked Windows 7/8 tool is the seemingly simple Calculator. It does much more than add/subtract/divide/multiply; Microsoft has effectively hidden the app's many advanced functions under the View menu. There you'll find options for scientific, programming, and statistical calculations. Even less known is a units-conversion screen associated with each type of calculator (see right). You can make quick conversions in 11 different units of measurement, ranging from Angle to Weight/Mass. There is also a related **Date calculation** which quickly gives you the number of days or the years/months/weeks/days between any two calendar dates, starting with the year 1700.



Select the type of unit you want to convert

Length

From

3

Kilometers

To

1.864113576712002

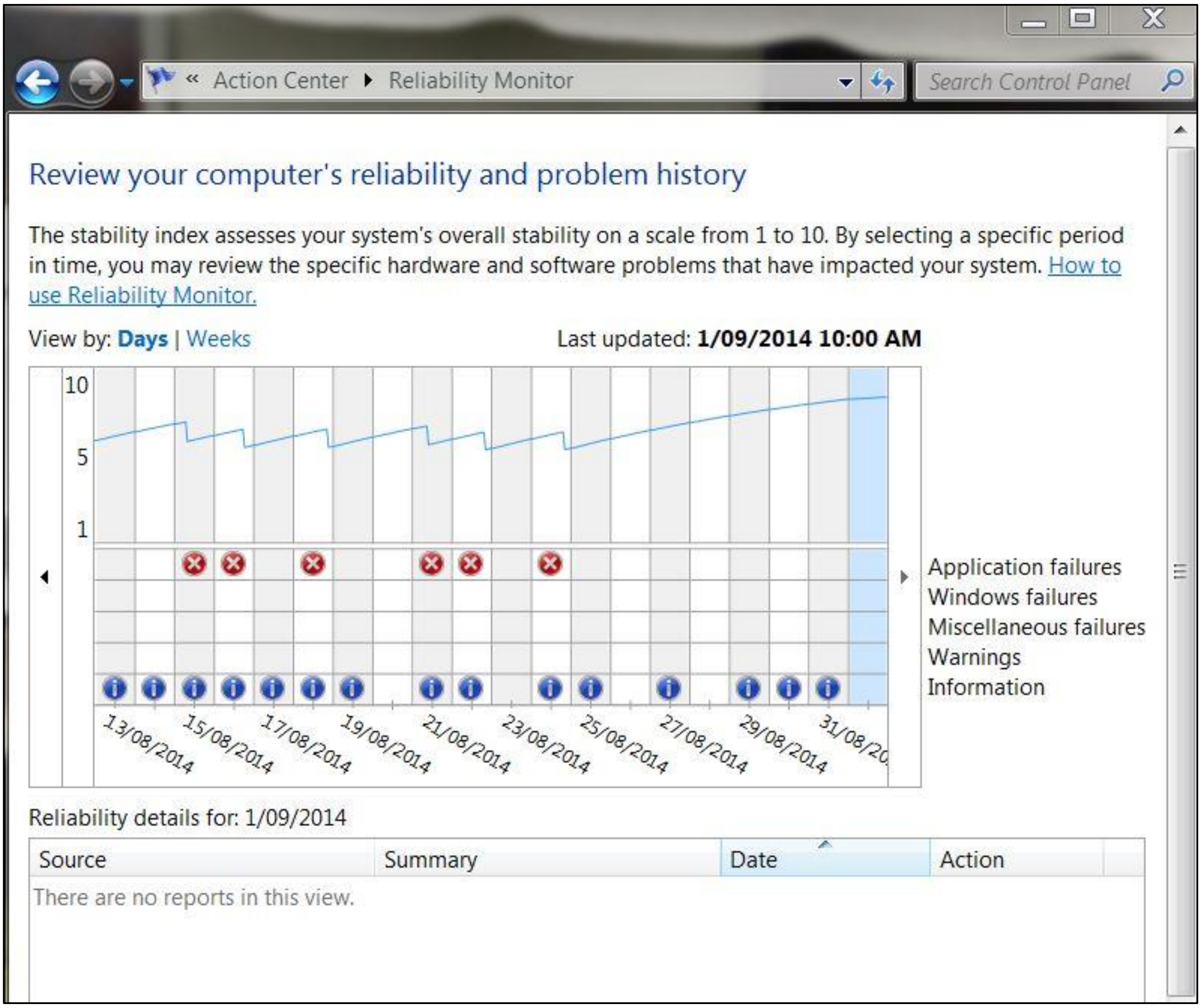
Mile

Clicking the Worksheets option lets you calculate mortgages, vehicle leases, or fuel economy.

Track Windows problems with Reliability Monitor.

When Windows freezes or an application suddenly stops working, the event is logged by the operating system. It can be difficult to troubleshoot those failures, but Windows' built-in Reliability Monitor can help. The Reliability Monitor resides under Windows' Action Center, but the easiest way to find it is via Windows' search bar. (It's included under the Action Center section of the All-Commands folder we created earlier but oddly you won't find it in Windows' Administrative Tools folder.)

Click the **View reliability history** link to launch Reliability Monitor. After you click the link, the application will take a few seconds or minutes to generate a report. It then displays a graph based on date and a stability scale of 1 to 10. Below the graph, a details section lists events, failures, warnings, and other information triggered by applications and Windows. The Action column in the details list includes links to possible solutions.



Review your computer's reliability and problem history

The stability index assesses your system's overall stability on a scale from 1 to 10. By selecting a specific period in time, you may review the specific hardware and software problems that have impacted your system. How to use Reliability Monitor.

View by: **Days** | Weeks

Last updated: **1/09/2014 10:00 AM**

Reliability details for: 1/09/2014

Source	Summary	Date	Action
There are no reports in this view.			

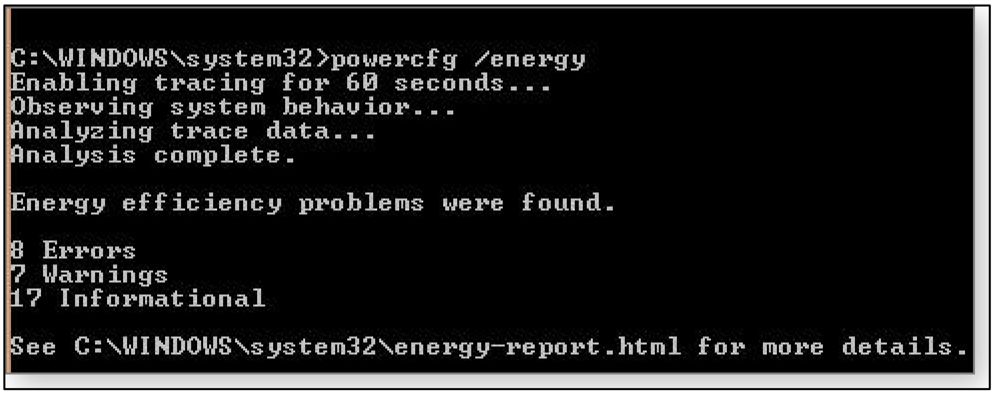
Here's a real-world application. After a recent update, my Windows 8.1 laptop kept freezing. The only solution was a hard reboot. A check with Reliability Monitor pinpointed Microsoft OneDrive as the culprit. Although the solutions link did not provide an answer, at least I knew the source of the problem — which gave me a starting point for possible fixes.

Powercfg utility traces laptop power woes

About 95 percent of the time, my work laptop is plugged into AC power. But recently, whenever I take it on the road, I invariably lose battery power quickly. (An HP portable, it can't be switched to hibernate mode.)

Activating Win7/8's **Power Efficiency Report** can help detect the root of power-management issues. Even if you don't think there's a power problem, running this report periodically is a great forewarned-is-forearmed strategy. To run a report, start at an administrator-level Windows command prompt. (Type **command** into the Windows search box. Right-click Command Prompt and select **Run as administrator.**)

Enter **powercfg /energy** at the prompt (include a space before the slash) and press Enter. Windows will take about a minute to assemble the report and then save it as **C:\Windows\System32\energy-report.html** (see right). Use Explorer's search box to locate the file quickly.



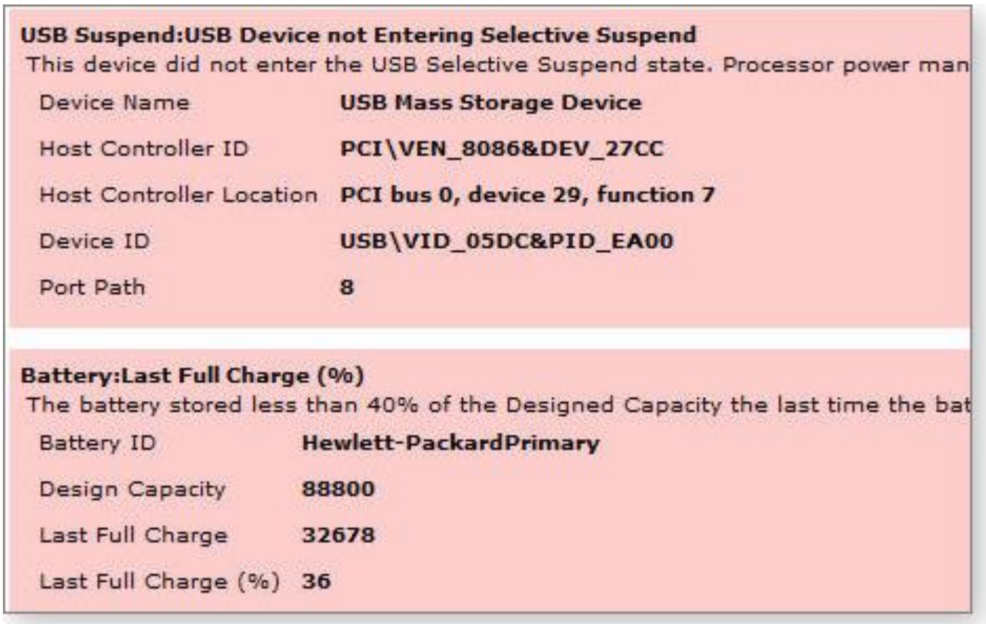
```
C:\WINDOWS\system32>powercfg /energy
Enabling tracing for 60 seconds...
Observing system behavior...
Analyzing trace data...
Analysis complete.

Energy efficiency problems were found.

8 Errors
7 Warnings
17 Informational

See C:\WINDOWS\system32\energy-report.html for more details.
```

The report will open in your default browser. Part of my report, which shows heaps of stuff, is shown below and provided the answer to my battery issue. The battery was charging to just 36 percent of its original capacity. No wonder I had to be near an AC outlet wherever I traveled with the machine. In addition to the aging battery, the report listed eight other errors and seven warnings. Most of those were remedied via adjustments to Windows' power-management tools.



USB Suspend:USB Device not Entering Selective Suspend

This device did not enter the USB Selective Suspend state. Processor power man

Device Name	USB Mass Storage Device
Host Controller ID	PCI\VEN_8086&DEV_27CC
Host Controller Location	PCI bus 0, device 29, function 7
Device ID	USB\VID_05DC&PID_EA00
Port Path	8

Battery:Last Full Charge (%)

The battery stored less than 40% of the Designed Capacity the last time the bat

Battery ID	Hewlett-PackardPrimary
Design Capacity	88800
Last Full Charge	32678
Last Full Charge (%)	36

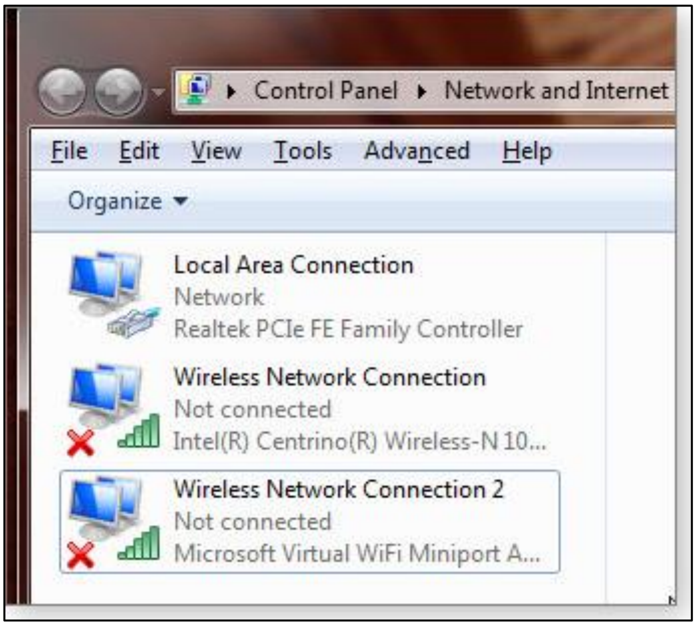
Win7's Virtual WiFi creates a free hotspot.

Most Windows 7 systems include the inconspicuous Microsoft Virtual WiFi Miniport adapter. It's a software-based access point that uses a wired or wireless connection to create a local hotspot.

This lesser-known feature is particularly handy, and economical, in locations in which you're charged for each Wi-Fi connection. With Virtual WiFi, multiple mobile devices can share one Internet connection.

To check whether your version of Windows supports virtual Wi-Fi, type **view network connections** into the Windows search box. Click the **View network connections** link and see whether **Wireless Network Connection 2** is listed. (The listing will also say **Microsoft Virtual WiFi Miniport Adapter.**)

Next, you'll need a third-party program to configure your hotspot. A popular application is Virtual WiFi Router (VWR) which you can get for free HERE. VWR is free however, to cover their costs they try and get you to download quite a few other programs. You can easily decline these.


Control Panel ▸ Network and Internet
File Edit View Tools Advanced Help
Organize ▾

Local Area Connection
Network
Realtek PCIe FE Family Controller

Wireless Network Connection
Not connected
Intel(R) Centrino(R) Wireless-N 10...

Wireless Network Connection 2
Not connected
Microsoft Virtual WiFi Miniport A...

BEFORE CELL PHONES AND SOCIAL NETWORKS
THIS IS HOW WE FIGURED OUT WHERE OUR FRIENDS WERE
imgflip.com

O

A woman runs a red traffic light and crashes into a man's car. Both of their cars are demolished, but amazingly, neither of them is hurt. After they crawl out of their cars, the woman says; "Wow, just look at our cars! There's nothing left, but fortunately we are unhurt. This must be a sign from God that we should meet and be friends and live together in peace for the rest of our days." The man replies, "I agree with you completely. This must be a sign from God!"

The woman continues, "And look at this, here's another miracle. My car is completely demolished, but my bottle of wine didn't break. Surely God wants us to drink this wine and celebrate our good fortune." She then hands the bottle to the man. The man nods his head in agreement, opens it, drinks half the bottle and then hands it back to the woman. The woman takes the bottle, immediately puts the cap back on, and hands it back to the man.

The man asks, "Aren't you having any?" The woman replies, "Nah. I think I'll just wait for the police."

Adam ate the apple, too. Men will never learn...