COMPUTER NEWS from the

JULY 2015 Volume3 NO. 7

As found on the web and other sources

Read This Before Selling Your Smartphone...

Category: Mobile From “askbobrankin.com”.

Before recycling, donating, or selling your smartphone, it’s a good idea to wipe it clean of all your contacts and other personal data. The easiest way to do that is the “factory reset” function; just tap it, confirm, and your phone is returned to the state it was in when it left the factory. All your personal data is gone. Or not. Read on to learn more...

Android Reset Vulnerability

The factory reset is supposed to scrub everything from your phone, and return it to "just out of the box" condition. Except your data isn’t gone completely, and much of it can be recovered by a tech-savvy snoop. Researchers at Cambridge University were able to recover passwords, contacts, photos, and other data that a factory-reset failed to erase from internal memory and external SD cards. Even full-disk encryption posed little hindrance to recovering "deleted" personal data.

The study, entitled Security Analysis of Android Factory Resets, included 21 smartphones from five manufacturers; the phones were running Android versions 2.3 to 4.3. (That means Android Gingerbread, Honeycomb, Ice Cream Sandwich, and Jelly Bean.) About 630 million such devices have been sold worldwide, and many have been re-sold or otherwise passed along.

The researchers say they don't know if more recent versions of Android have the same shortcomings. What??? They didn't test the two most recent versions of the operating system? (Android KitKat and Lollipop run on 50% of all Android devices.) That's just bizarre. But anyway, let's continue...

In 80% of the tested phones, researchers were able to recover the master token that Android uses to provide access to Google services such as Gmail, Calendar, etc. So when these phones were reset and rebooted, they immediately synced with Google services to recover all the data stored there: emails, appointments, contacts, even text messages and voicemails. Tokens for other apps, including Snapchat and Facebook, were also recoverable on a majority of tested phones.

In case that's not clear, it means that in addition to recovering the data left on your phone, a determined hacker could gain *ongoing access* to your online accounts. So by all means change your passwords if you lose or sell a phone.

Why is it So Hard to Wipe a Phone?

iPhone users can wipe that smug look off their faces… The Cambridge researchers didn't test to see if iPhones and iPads are similarly vulnerable. AND... It's just been found that a specially crafted text message, sent from another phone, can shut down your iPhone. Fortunately, there's a way to protect your iPhone, until a better fix is released by Apple.

Part of the problem is that some manufacturers do not include with their phones the software drivers needed to wipe non-volatile external storage devices, such as SD cards. But the main problem is internal flash memory, which is notoriously difficult to "wipe" completely.

Surprisingly, the researchers found that the “crypto footer” file which stores the decryption key of a fully encrypted flash drive is not erased during a factory-reset. This key is generated by the combination of a semi-random system-generated “cryptographic salt” value and a user-defined PIN or password. Since users tend to choose weak PINs and passwords, the crypto footer is easily cracked in less than a day, according to Kenn White, a North Carolina computer scientist.

The Cambridge study’s findings put Android users in a predicament when they want to dispose of a used phone, or when a phone is lost and a remote wipe is advisable. If full-disk encryption is available, it’s best to use it and choose a strong password: one that incorporates alphabetical, numeric, and special characters, and is more than 11 characters long. But given how often people need to unlock their phones and the challenges of smartphone keyboards, strong passwords are not likely to be used by many.

As for third-party remote-wiping apps, the same researchers also published a study entitled, Security Analysis of Consumer-Grade Anti-Theft Solutions Provided by Android Mobile Anti-Virus Apps. It found significant wiping flaws in 10 Android apps that have been downloaded hundreds of millions of times.

The bottom line: Encrypting your phone with a complex password before you do a factory reset will make it much harder (but not impossible) for a determined person to recover your data. The only way to ensure that your data doesn’t fall into the wrong hands is to destroy a used phone instead of reselling or donating it. That’s little comfort for people who lose phones. If you've sold or lost an Android-powered phone, the best you can hope is that it doesn't end up in the hands of a tech-savvy snoop.

Vampire power costs Americans $19 billion in electricity every year

Megan Treacy (@mtreacy) in “treehugger.com”.

Energy / Energy Efficiency

The typical American home is full of vampires. Vampire electronics that is. These always-on devices suck up electricity even when we're not using them and the more wired and connected we make our lives, the greater the amount of vampires we end up with.

A new **report from the National Resource Defense Council** states that Americans are spending $19 billion a year in electricity costs from vampire appliances and electronics. That comes down to $165 per household on average, but could cost as much as $440 per household under top-tier rates. The annual power usage is equal to the output of 50 large power plants and an equal amount of emissions.

"One reason for such high idle energy levels is that many previously purely mechanical devices have gone digital: Appliances like washers, dryers, and fridges now have displays, electronic controls, and increasingly even Internet connectivity, for example," says Pierre Delforge, the report's author and NRDC's director of high-tech sector energy efficiency. "In many cases, they are using far more electricity than necessary."

Two major offenders that we've discussed before are **TV cable boxes** and video game consoles. Cable boxes are the second largest energy user in many people's homes because they are always running even when they are turned off thanks to spinning hard drives, program guide updates and software downloads. **Video game consoles** can be major power hogs and the systems' stand-by modes leave much to be desired. Many users are reluctant to shut them off completely because restarting them can take such a long time when updates have to be installed.

While studies have focused on these individual electronics in the past, the NRDC study is the first to analyze the impact of all the idle electronics in our lives. The group looked at energy usage data from electric utility smart meters in 70,000 northern California homes as well as field measurements that concentrated on idle loads. They found an average of 65 vampire power loads in homes, including things like appliances, devices in standby mode (even things like garage door openers), electronics in sleep mode like game consoles and TVs, and devices like computers that are left fully on, but are not in use.

The always-on devices consumed an average of 164 watts per home, the same as brewing 234 cups of coffee every day for a year (more than 85,000).

The good news is that making improvements in your idle power load is easy.

"Consumers can take such steps to reduce their idle load as **using timers**, smart power strips, and changing settings on their devices, and manufacturers need to do their part by designing products to minimize energy waste, but ultimately policies like energy efficiency utility programs and standards are needed," Delforge notes. "Reducing always-on consumption is a low-hanging fruit opportunity to cut climate-warming pollution."

If you want some specific pointers, the NRDC did the hard work for us and put together this great list of actions for identifying and reducing your vampire power loads **here (PDF)**.

The Other Search Engines

Category: Search-Engines In “askbobrankin.com”.

We’re used to thinking of the Big Three in search engines: Google, Microsoft Bing, and Yahoo! But on a global level, there’s a Big Four. And there are plenty of smaller search sites vying for attention. Here's what you need to know about alternative search engines…

Whales in the Fishtank

In the USA and most of the world, Google has a commanding lead in search, handling about 65% of all queries. Along with Microsoft Bing (20%) and Yahoo (13%), these three comprise 98% of the search market share.

On a global scale, there's a huge fourth player in the search game. Baidu (BY-doo) is a Chinese Web services firm that was incorporated in 2000. Search is only part of its business, just as its only part of Google’s business. Baidu also has social networks, and a Wikipedia-style online encyclopedia.

Baidu is second only to Google in the number of search queries processed with 13%, according to the April, 2015, figures released by research firm Net Market Share. And in China, Baidu has a 56% share of the more than 4 billion searches conducted each quarter. With Baidu in the mix, Bing and Yahoo! are tied for third place with 9% each.

So what's left? The combined market share of AOL, Ask.com, and Lycos is under 1%. The “Other” category (about 1.5% of all searches) is chock full of search engines you’ve probably never heard of (unless you’ve been reading me for several years).

The continued existence of Lycos surprises me. Once a pioneer of Internet search, Lycos vanished from most people's radar about ten years ago. Headquartered in Massachusetts, Lycos has only 72 U. S. employees. Since 2010, it has been owned by India's Internet marketing firm, Ybrant Digital.

In my opinion, Wolfram Alpha is the most important search engine in that "other" category, because its unique "calculated answers" technologies are licensed by Google, Bing, and Yahoo! But you can access Wolfram Alpha directly, too.

What Else is in the "Other" Category?

What is a REAL Search Engine? I don't think AOL should be considered a "search engine." Its results all come from Google, with some AOL content thrown in for ad revenue. I could say the same about Yahoo, which has a checkered history as a search engine. Starting in 2001, Yahoo search results were provided by Inktomi, now defunct. They used Google for a few years, and then went "legit" in 2004, creating their own search engine technology and web index. But since 2009 it has been "powered by Bing."

I would not use Ask.com to find a nearby hospital even if my femoral artery was spurting blood clear across the street. It's owned by InterActive Corp., maker of adware, bogus dating sites, and the infamous Ask.com Toolbar.

Even more on the fringe of popularity are "privacy enhancing" search sites like IxQuick, Startpage, and DuckDuckGo. These sites promise not to share your IP address or personal information with other sites or advertisers. IxQuick and DDG query several search engines and present the top results. StartPage acts as an anonymous proxy to Google.

Some call these sites privacy heroes, but I see them in a more nuanced way. None of them do the "heavy lifting" required to scan and index the World-Wide Web, but they paint those who do (primarily Microsoft and Google) as villains, and profit from their work. Personally, I have no qualms with the privacy policies of Google or Microsoft, and believe that much of the talk on this subject is hype or hyperbole. (See Is Google's Privacy Policy Evil? and Google Security and Privacy Dashboard.)

In addition to general search sites like these, there is a myriad of searchable databases, directories, and Wikis. Some of the most useful and popular ones are:

The Internet Movie Database was started in 1990 by computer programmer Col Needham to index, rate, and discuss movie titles, characters, production staff, and stars. It proved to be a blockbuster idea, and the database was expanded to include TV programs and even video games. In 1998, the IMDB was acquired by Amazon.com, a natural fit for a company that sells digital entertainment.

Wikipedia has singlehandedly decimated the paper encyclopedia industry, with the full approval of tree fans. The collaborative encyclopedia ranks among the top ten sites on the Internet, and is widely considered the most-used reference resource online.

Quora combines a database of writings on many topics with a community of users who may be just the experts, mentors, or sources that you need. You can post questions and helpful experts will answer them.

Dogpile is a “meta-search tool.” It queries multiple search engines and online databases to answer your inquiries.

While it’s handy and simple to “just Google it,” you may also want to check out some specialized searchable resources. Do you have a favorite "alternative" search site?

Every 4 Seconds New Malware Is Born

By *Ericka Chickowski in “darkreading.com”.*

New report shows rate of new malware strains discovered increased by 77 percent in 2014.

New research data out today shows that the rate of new malware variants released by malicious attackers continues to break records. According to the G DATA SecurityLabs Malware Report, new malware types were discovered less than every four seconds and 4.1 million new strains were found in the second half of 2014, an increase of close to 125 percent over the first half. Over the course of the entire year, nearly 6 million new malware strains were discovered. This is a 77 percent increase over 2013.

The data shows that in the second half of 2014, Trojans still remained atop the categories tracked by G DATA researchers, but could be on pace to be supplanted by adware. Adware showed the highest rate of growth among all of the malware categories, at a rate of 31.4 percent. While the number of new downloaders was on the rise during the second half, adware's growth rate outpaced that rise to take over the number two spot on the malware category chart. Meanwhile, spyware increased in prevalence while backdoors decreased; putting them in the number four and five spot, respectively.

Interestingly, while rootkits ranked ninth in the categories list, the second half of the year saw a huge spike in their prevalence. The report showed that there were 18 times more new variants than in the first half of 2014.

Specifically within the Trojan market, researchers reported that the second half of the year was novel in that there were no significant innovations compared to previous years.

"In the past, more and more new Trojans have been appearing very quickly in this sector over the years, with new groups in the background using new attack methods. However, in recent months there have been few changes to report," the study said, explaining that in spite of this the volume of attacks is still rising. According to G DATA, the number of banking Trojan attacks rose by 44.5 percent.

The authors speculated that the banking Trojan market seems to have consolidated due to a number of reasons.

"Improved security measures by banks are making it more and more difficult for online bank robbers to get money from bank customers," explains Ralf Benzmüller, head of G DATA SecurityLabs.

Some of the factors at play include an increase of criminal prosecutions against attackers, improved two-factor authentication measures and greater dependence by banks on anomaly detection to reduce fraud. As researchers explained, there's an increased risk for criminals and

fraud takes more effort for lower yield. There's also a higher barrier to entry as attacks take "a certain amount of expertise and infrastructure" to carry out.

Ericka Chickowski specializes in coverage of information technology and business innovation. She has focused on information security for the better part of a decade and regularly writes about the security industry as a contributor to Dark Reading. *View Full Bio*

I WENT TO A BOOKSTORE AND ASKED THE SALESWOMAN, "WHERE'S THE SELF- HELP BOOKS?

SHE SAID IF SHE TOLD ME, IT WOULD DEFEAT THE PURPOSE.

And finally

Why doesn’t your dog or cat recognize your face on a smartphone screen? Scientists say dogs see differently, while cats just don’t give a darn about you.