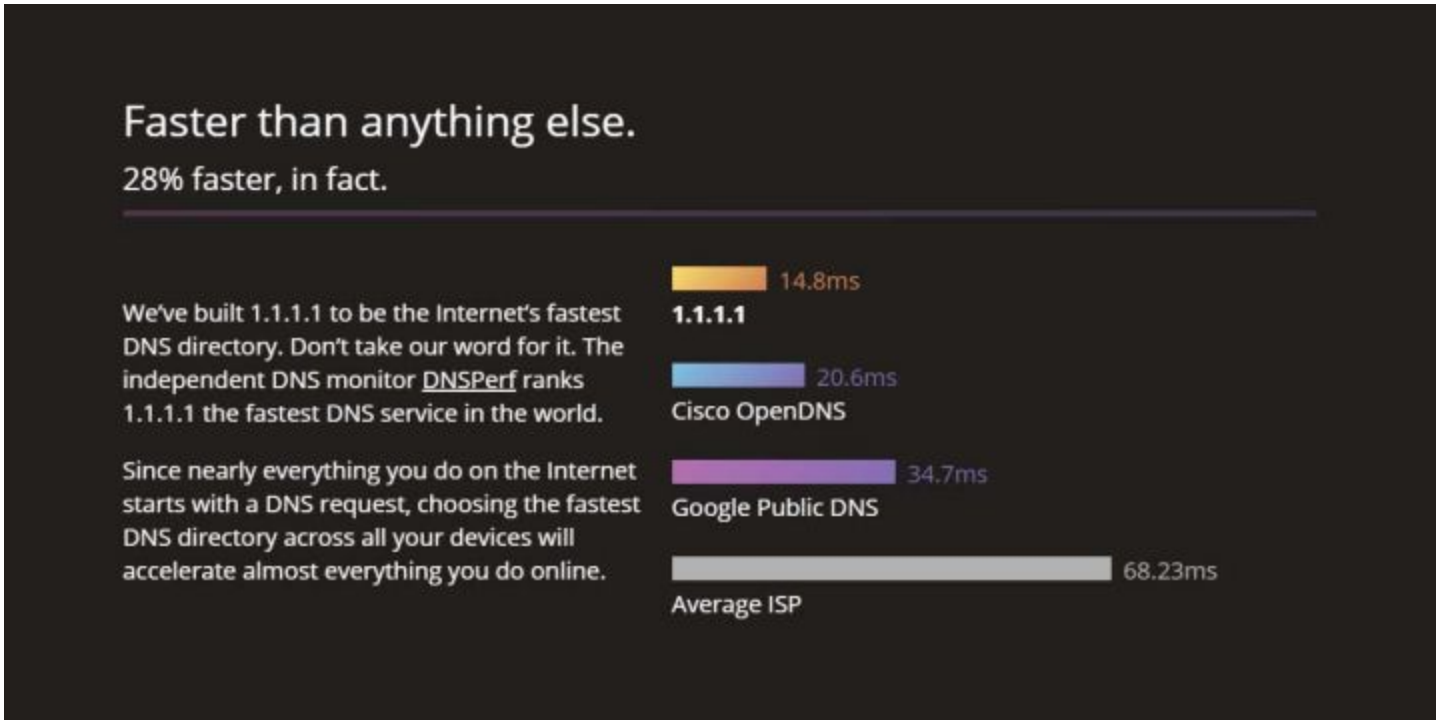
Security Now! #657 - 04-03-18

ProtonMail

This week on Security Now!

This week we discuss "DrupalGeddon2", Cloudflare's new DNS offering, a reminder about GRC's DNS Benchmark, Microsoft's Meltdown meltdown, the persistent iOS QR Code scanner flaw, iOS's much anticipated v11.3 update, another VPN user-IP leak, more bug bounty news, an il-fated-seeming new eMail initiative, the consequences of free electricity, a policy change at Google's Chrome store, another "please change your passwords" after another website breach, a bit of miscellany, a heart warming SpinRite report, some closing the loop feedback from our terrific listeners, and a closer look at the Swiss encrypted ProtonMail service.

Our Picture of the Week



Security News

Drupalgeddon2 Allows Hackers to Take Over Sites
Last Wednesday, as planned and pre-announced, the Drupal team released patches for current and previous releases of Drupal, including the v6.x branch which was discontinued more than two years ago.

The flaw allows unauthenticated remote code execution (RCE).

Even Drupal's own site was taken down shortly after the release of the updates so that it, too, could be updated.

What do we know?
The bug (designated CVE-2018-7600) allows an attacker to run any code desired against Drupal's core component, effectively taking over the site.

The attacker doesn't need to be registered or authenticated on the targeted site and all the attacker must do is to access an URL.

The Drupal community has dubbed this bug "Drupalgeddon2" because "Drupalgeddon" was already taken by the super-severe bug (CVE-2014-3704, SQL injection, severity 25/25) disclosed in 2014... which led to unpatched Drupal sites getting hacked for years afterward.

Jasper Mattsson, an employee of Drupal security auditing firm Druid, is credited with the bug's discovery.

The flaw has been described as “an input validation issue where invalid query parameters could be passed into Drupal webpages.” and no Proof of Concept code was released since no one wearing a white hat wants to provide those with malicious intent any leg up on this one.

The fact that the much older v6.x branch was also affected suggests that the bug has been present for a long time.

According to BuiltWith.com, Drupal currently powers over one million sites and has a 9% market share among the top 10K most popular sites.

Greg Knaddison, a Drupal security team member, said the vulnerability has to do with the way Drupal interprets a value that begins with a hash as having a special meaning.

Knaddison said there are a number of strong indicators that Drupal users are getting a jump on patching. He estimates “hundreds of thousands” of sites immediately patched within the first 12 hours the patches were released.

But according to an analysis of Drupal sites by the firm SiteLock, only 18 percent of Drupal websites were found to be running the latest core updates. This suggests that the vast majority of websites running Drupal are likely vulnerable to compromise because they are not being updated with the latest security patches.

Cloudflare 1.1.1.1 - Launches Publicly DNS-Over-HTTPS Service
Last week's podcast, which talked about Mozilla and Cloudflare teaming up to introduce and support DoH (DNS over HTTPS) preceded Cloudflare's big Easter Sunday April 1st (non April Fool's) announcement of their new "Quad One" DNS service.

1.1.1.1 -and- 1.0.0.1 → But note that 1.0.0.1 is significantly slower (how much slower? see GRC's DNS Benchmark) and is only intended to be used as a backup. So be certain that 1.1.1.1 is the first-listed Primary DNS.

Olafur Gudmundsson, director of engineering at Cloudflare, said: "Our goals with the public resolver are simple: Cloudflare wants to operate the fastest public resolver on the planet while raising the standard of privacy protections for users."

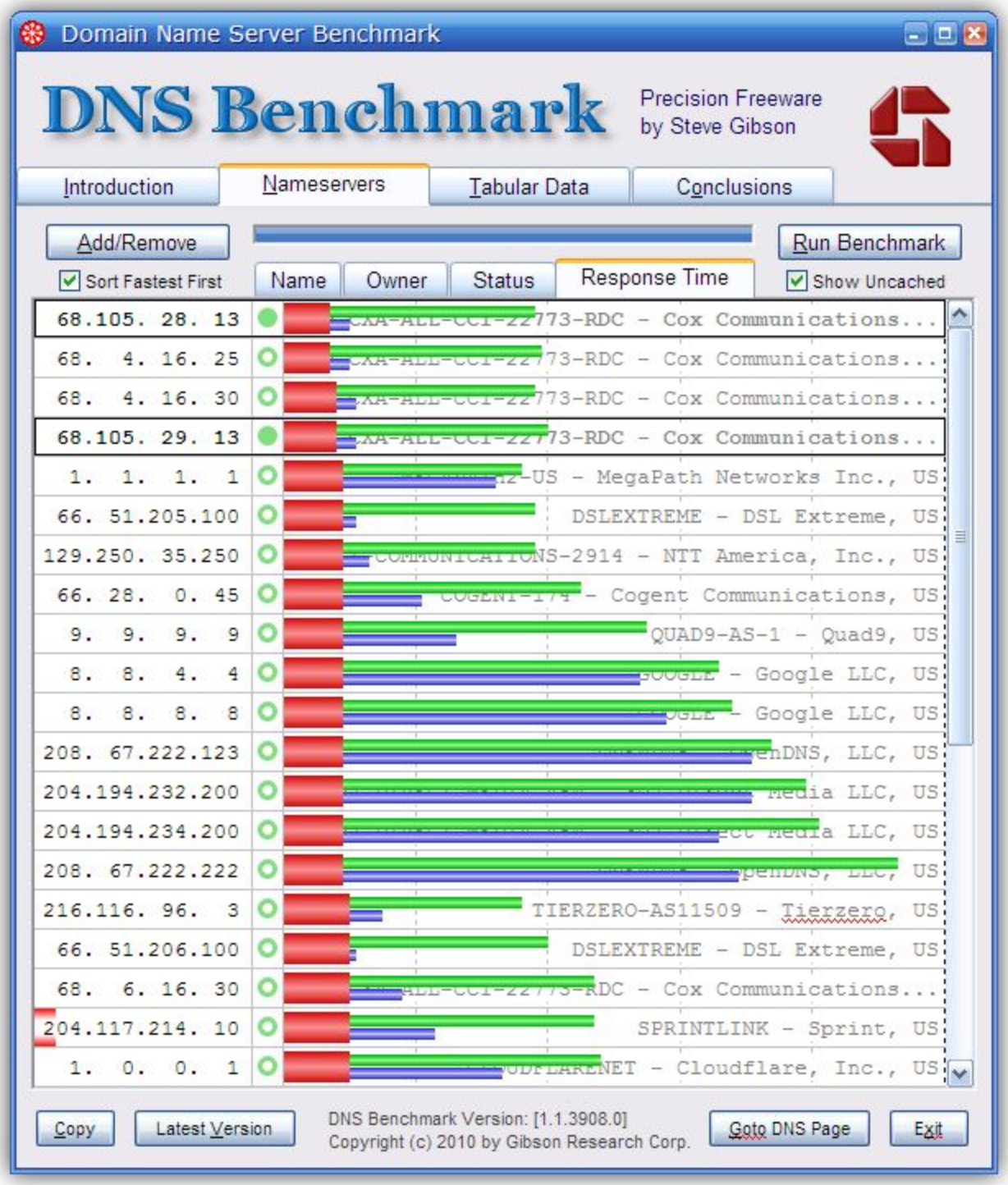
He said: "We began talking with browser manufacturers about what they would want from a DNS resolver. One word kept coming up: privacy. Beyond just a commitment not to use browsing data to help target ads, they wanted to make sure we would wipe all transaction logs within a week. That was an easy request. In fact, we knew we could go much further. We committed to never writing the querying IP addresses to disk and [to] wiping all logs within 24 hours."

The DNS resolver, 1.1.1.1, is also supporting privacy-enabled TLS queries on port 853 (DNS over TLS), so we can keep queries hidden from snooping networks. Furthermore, by offering the experimental DoH (DNS over HTTPS) protocol, we improve both privacy and a number of future speedups for end users, as browsers and other applications can now mix DNS and HTTPS traffic into one single connection.

With DNS aggressive negative caching, as described in RFC8198, we can further decrease the load on the global DNS system. This technique first tries to use the existing resolvers negative cache which keeps negative (or non-existent) information around for a period of time. For zones signed with DNSSEC and from the NSEC records in cache, the resolver can figure out if the requested name does NOT exist without doing any further query. So if you type wwwwwww dot something and then wwww dot something, the second query could well be answered with a very quick "no" (NXDOMAIN in the DNS world). Aggressive negative caching works only with DNSSEC signed zones, which includes both the root and a 1400 out of 1544 TLDs are signed today.

We use DNSSEC validation when possible, as that allows us to be sure the answers are accurate and untampered with. The cost of signature verifications is low, and the potential savings we get from aggressive negative caching more than make up for that. We want our users to trust the answers we give out, and thus perform all possible checks to avoid giving bad answers to the clients.

However, DNSSEC is very unforgiving. Errors in DNSSEC configuration by authoritative DNS operators can make such misconfigured domains unresolvable. To work around this problem, Cloudflare will configure "Negative Trust Anchors" on domains with detected and vetted DNSSEC errors and remove them once the configuration is rectified by authoritative operators. This limits the impact of broken DNSSEC domains by temporarily disabling DNSSEC validation for a specific misconfigured domain, restoring access to end consumers.



How to configure GRC's DNS Benchmark:

1. Launch the DNS Benchmark.
2. Click on the "Nameservers" tab -and- wait for the initialization to complete.
3. Click the Add/Remove button at the left below the tabs.
4. Enter "1.1.1.1" and click "Add"
5. Enter "1.0.0.1" and click "Add"
6. Click "Run Benchmark"
7. While it's running, stretch the window to the top and bottom of your screen.
8. When completed, left click on the results and drag the mouse to show numerical timing.

Windows Meltdown Patch Patch
Swedish security researcher (Ulf Frisk), developer of the PCILeech Kernel memory hacking tool, discovered that Microsoft's January 2018 patch for Windows 7 64-bit OSes mistakenly flipped a Supervisor Mode/User Mode permission bit which has, since then, been allowing any app to read or write data from/to the affected OS's kernel memory.

Late lack week Microsoft pushed out an out-of-cycle emergency update to flip this wayward kernel memory access-control permission-bit back to where it was supposed to be.

The flaw is not (or was not) remotely exploitable, and attackers need either physical access to a PC, or they need to infect the PC with malware beforehand.

Win7/64 (and Server 2008 R2) users may wish to be sure they have KB4100480 installed.

Ulf Frisk's PCILeech, which describes itself as Direct Memory Access (DMA) Attack Software (Google" "PCILeech") may also be used to check for this vulnerability... though it might also Blue-Screen a vulnerable system. So be prepared to reboot.

https://github.com/ufrisk/pcileech

And speaking of bugs and patches...
The much covered iOS QR Code flaw was NOT fixed by the long-awaited v11.3 mega update.

This is a bit surprising since it's a worrisome QR Code spoofing bug that Apple has presumably known of since December 23rd, 2017 when it was reported to Apple by Roman Mueller who first discovered the flaw.

90 days later, still unpatched, Roman published his findings.

With iOS v11, the iOS camera app is continually looking for QR codes and, when found, displays a confirmation message prompting the user whether they wish to open Safari at that URL. But there's a URL parsing error which allows the true URL domain to be hidden behind a spoofed display URL. By exploiting the URL parsing flaw one domain can be shown while another entirely different domain is visited. What Mueller discovered was that the iOS camera's QR code interpreter misreads certain URL formats, selecting for display a different portion of the specially crafted URL than Safari. That difference can be exploited to take even vigilant users to malicious domains.

https://xxx\@facebook.com:443@infosec.rm-it.de/

It's difficult to understand why this hasn't been fixed. Among the many problems repaired by last week's release of iOS v11.3 was a bug in Safari about which Apple writes: "For: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation. Impact: Visiting a malicious website by clicking a link may lead to user interface spoofing. Description: An inconsistent user interface issue was addressed with improved state management.

Yeah... and the QR Code interpreter could also use a bit of that.

And speaking of the iOS v11.3 mega-update...
Released last week, v11.3 fixes 43 different known security vulnerabilities.

watchOS v4.3 resolves 22 problems, tvOS v11.3 fixes 28, and Xcode v9.3 fixes one.

The only additional thing to be said is that not a single one of my previously up to date iPhones or iPads -- about eight in total -- had thought to prompt me for updating. When I went to check manually each one was eager to bring themselves current... but I had to ask. So if you are an iOS user and you don't know that your devices have updated since the middle of last week (around March 27th) you should give your devices a bit of a kick.

And we have another VPN client-IP leak...
A well-known WebRTC IP leakage problem, which has been known since January 2015, is not being filtered and eliminated by a worrisome number of VPN providers.

Paolo Stagno, a security researcher who uses the handle "VoidSec" audited 83 VPN apps to see whether they were properly anonymizing their users by filtering this longstanding WebRTC IP leak. He found that of those 83 he checked, 17 VPN systems were still leaking their user's IP addresses.

Stagno says he found that 17 VPN clients were leaking the user's IP address while surfing the web via a browser.

Since he was unable to test every VPN system, especially commercial offerings, Paolo setup a nice self-help testing web page will be allow anyone using a VPN to determine, either way, whether their IP is accessible while surfing web pages.

https://ip.voidsec.com/

https://docs.google.com/spreadsheets/d/1Nm7mxfFvmdn-3Az-BtE5O0BIdbJiIAWUnkoAF_v_0ug/edit#gid=0

"HotSpot Shield" does NOT leak.
"HideMyAss" =does= leak!

The US DoD gets into the Bug Bounty craze...
https://www.businesswire.com/news/home/20180402005247/en/U.S.-Department-Defense-Kicks-Bug-Bounty-Challenge

DoD Bug Bounty program, registration open from April 1st through April 29th.

HackerOne
General Motors, Lufthansa, Starbucks Coffee, EU, Spotify, AirBNB, Lending Club, Nintendo, Wordpress, Twitter, Shopify, Ghostery, Google Play, Cylance

https://hackerone.com/hacktivity?sort_type=popular&filter=type%3Aall&page=1&range=forever

Jack Messer, project lead at Defense Manpower Data Center said: "The Department of Defense enterprise system is relied on by millions of employees for global operations. The DoD has seen tremendous success to date working with hackers to secure our vital systems, and we're looking forward to taking a page from their playbook. We're excited to be working with the global ethical hacker community, and the diverse perspectives they bring to the table, to continue to secure our critical systems."

To be eligible to participate in the bug bounty challenge, individuals from the public must be United States taxpayers or a citizen of or eligible to work in the United Kingdom, Canada, Australia, or New Zealand. U.S. government active military members and contractor personnel are also eligible to participate but not eligible for financial rewards. See full eligibility requirements...

History:
Since the "Hack the Pentagon" program kicked off in 2016, over 3,000 vulnerabilities have been resolved in government systems:

The first "Hack the Air" Force bug bounty challenge resulted in 207 valid reports and hackers earned more than $130,000 for their contributions.

The second "Hack the Air Force" resulted in 106 valid vulnerabilities surfaced and $103,883 was paid to hackers.

"Hack the Army" in December 2016 surfaced 118 valid vulnerabilities and paid $100,000.

"Hack the Pentagon" in May 2016 resulted in 138 valid vulnerabilities resolved and tens of thousands paid to ethical hackers for their efforts.

"Hack the Air Force 2.0" demonstrates continued momentum of the Hack the Pentagon program beyond just its first year, as well as a hardened attack surface.

I really like the idea of companies paying for the discovery of important bugs in their systems and this evolving model where talented freelance computing enthusiasts can earn real money by searching for, discovering and responsibly reporting bugs in high profile software.

BIMI: "Brand Indicators for Message Identification"
https://www.brandindicators.org/
https://authindicators.github.io/rfc-brand-indicators-for-message-identification/

The "Authindicators Working Group"
Members include Agari, Comcast, Google, LinkedIn, Microsoft, Oath (the Verizon subsidiary that operates AOL and Yahoo), PayPal, Returnpath and Valimail.

"What If You Could Put Your Brand On Every Email …and Users Could Trust It's You?"

From the site: "Brand Indicators for Message Identification (BIMI) is an industry-wide standards effort that will use brand logos as indicators to help people avoid fraudulent email, while giving marketers a huge new opportunity to put their brands in front of consumers for free. If you use Yahoo Mail, you will see brand indicator logos from Groupon, Agari and other large brands in the financial services, aviation and technology industries."

Brand Impression
Every time you send an email, you are guaranteed your logo will be displayed in the preview pane and near the "from" line.

Trusted Communications
When users see your logo, they'll trust the email and be more likely to do respond to your email and do business with you.

Stop Phishing
Brand Indicators will authenticate the sender of the email using an existing standard (DMARC) before displaying your logo.

But… From the specification under "3.2. Security"...

Brand indicators are a potential vector for abuse. BIMI creates a relationship between sending organization and Mail Receiver so that the receiver can display appropriately designated indicators if the sending domain is verified and has meaningful reputation with the receiver. Without verification and reputation, there is no way to prevent a bad actor exxample.com from using example.com's brand indicators and behaving in a malicious manner. This document does not cover these verification and reputation mechanisms, but BIMI requires them to control abuse.

Free Electricity?
Cryptocurrency mining might be expected to pop-up anywhere you have savvy techies and free electricity... such as in any University setting where students are not responsible for paying for their personal electrical use.

An online posting titled: "University found out I'm mining bitcoin in my dorm" reads:
I have free electricity here at ASU and I decided to use Nice Hash to min some bitcoin. I've been mining for a month with no problems with a pair of GTX1080TI's. But I just received an eMail today that I need to uninstall my mining hardware. Now, I am pretty sure this is not based off my electricity bill as I mined with my laptop for a bit at the same time and they said I had two devices mining. Now I am wondering how I can get around this problem? Should I use a VPN? Or is there another way to disguise my mining?

No more mining in Chrome
https://blog.chromium.org/2018/04/protecting-users-from-extension-cryptojacking.html
Meanwhile, BleepingComputer reports that Google has announced that effective yesterday, April 2nd, the Chrome Web Store review staff has stopped accepting new extensions on the Web Store that perform cryptocurrency mining operations. And that existing Chrome extensions that perform cryptocurrency mining will be delisted sometime in late June.

Until this policy change yesterday, Google allowed extensions to mine cryptocurrencies only if cryptocurrency mining was the extension's sole purpose, and if the user was informed in advance that their computer's resources were going to be used for this hardware-intensive task.

James Wagner, Extensions Platform Product Manager for Google said "Unfortunately, approximately 90% of all extensions with mining scripts that developers have attempted to upload to Chrome Web Store have failed to comply with these policies."

In other words... nearly all Chrome extension based mining is cryptojacking.

Remember that Chrome includes its own Task Manager located under "More Tools" that will show the percentage of CPU being consumed for each of its own tabs.

Under Armour App Breach Exposes 150 Million Records
A breach in a database for MyFitnessPal exposes the logon information for 150 million users. Username, eMail and hashed passwords were stolen.
But no credit card or other information appears to have been accessed since that's stored in a non-breached database.

So the protocol is what we've become accustomed to after breaches:
We don't have details of how strongly protected the password hashes were.
So users of "MyFintnessPal" should change their password (and make it strong while you're at it.) And anywhere else that the same password was used should be changed as well.

Miscellany
Star Trek: Discovery was definitely worth the watching.

SpinRite

Dan Martins in Fairbanks, Alaska
SpinRite did it again!

Dear Steve, I'm writing to pass along my mother's ecstatic joy and thanks for what SpinRite did for her. I have been listening to you and Leo for years and I purchased SpinRite mostly to support you and everything you do for us. I've used it from time to time to check on the drives in my systems and it may have ben helping to keep everything working without any trouble as we know it can.

However, my mother's computer did not have SpinRite's maintenance help and it died without warning. Well, really, there was warning, but she did not know to read the signs. She explained that it had been taking longer and longer to start up in the morning, but she heard that computers slowed down. So she figured that was normal. And, naturally, she had not backed up about three months worth of work on the sequel to her first novel. The copy she had on a thumb drive would not read back, and it looked like a complete loss.

Since I am my family's go-to computer tech, she called in a panic and explained that she and her husband had tried everything and they feared the worst. But I knew one thing they had not tried.

Her computer has a DVD, so I created and sent her a bootable SpinRite CD. After it arrived I helped them start SpinRite running and told them to call me back when it was finished.

Since I've been listening to you and Leo for years, we all know how this story ends. When she rebooted her computer, everything was back to full speed like it was new, and more importantly, her nearly finished second novel was completely readable. She couldn't believe it... but I knew to expect it. Having had a "near death" experience, she will be backing up to multiple drives from now on.

So a happy Easter was had, and "thank you" hardly seems like enough.

Your avid listener and supporter,
Dan.

Closing The Loop

"Doug J" / Subject: COBOL

Hello Steve,
Unfortunately, COBOL is still the old and crumbling foundation for PeopleSoft.
I dread it because the once a year I have to look at it and hope I do not have
to make some change (fearing unintended consequences)...

(... PeopleSoft, now owned by Oracle:
PeopleSoft, Inc. was a company that provided human resource management systems (HRMS),

Financial Management Solutions (FMS), supply chain management (SCM), customer relationship management (CRM), and enterprise performance management (EPM) software, as well as software for manufacturing, and student administration to large corporations, governments, and organizations. It existed as an independent corporation until its acquisition by Oracle Corporation in 2005. The PeopleSoft name and product line are now marketed by Oracle.

PeopleSoft Financial Management Solutions (FMS) and Supply Chain Management (SCM) are part of the same package, commonly known as Financials and Supply Chain Management (FSCM).

From: "Greg V"
Subject: Cloudflare's quad-1s and privacy?

Steve,

If DNS UDP traffic passes through your ISP unencrypted, how can it be "private"? Isn't it a simple task for the ISP to track the queries?

Spinrite owner,
Greg

Scott T on the East Coast
Subject: Secure Email / Trasnition away from Gmail
:
I am looking to move away from Google Mail and was wondering what options you recommend besides spinning up your own server, or if you do recommend spinning up your own server, what's the best way to make it as maintenance free as possible.

Thanks, Keep up the good work.
Scott T..

ProtonMail

https://protonmail.com/

ProtonMail's iOS and Android mobile apps now allow users to store sensitive contact information.
https://protonmail.com/blog/mobile-encrypted-contacts/
Until now this feature was desktop/web only. But now this has been added to the mobile apps.

What is Proton Mail?

It's an end-to-end encrypted email service founded in 2014 at the CERN research facility in Switzerland.

On the desktop, ProtonMail offers web browser JavaScript-driven client-side encryption to protect email contents in flight and stored. It also offers iOS and Android apps.

ProtonMail is operated by Proton Technologies AG, a company based in the Canton of Geneva with servers in two locations in Switzerland, both outside of US and EU jurisdiction.

The default account setup is free and the service is sustained by optional paid services. As of January 2017, ProtonMail had over 2 million users.

Anonymous Email / Protect Your Privacy
No personal information is required to create your secure email account. By default, we do not keep any IP logs which can be linked to your anonymous email account. Your privacy comes first.

Open Source / Free Secure Email
We believe email privacy should be available to all. That's why our code is open source, and basic ProtonMail accounts are always free. You can support the project by donating or upgrading to a paid account.

Easy to Use / Security without the hassle
ProtonMail can be used on any device without software install. ProtonMail secure email accounts are fully compatible with other email providers. You can send and receive emails normally.

Physical Security
ProtonMail's infrastructure resides in Europe's most secure datacenter, underneath 1000 meters of solid rock.

Encryption
ProtonMail uses a combination of public-key cryptography and symmetric encryption protocols to offer end-to-end encryption. When a user creates a ProtonMail account, their browser generates a pair of public and private RSA keys:

- The public key is used to encrypt the user's emails and other user data.

- The private key capable of decrypting the user's data is symmetrically encrypted with the user's mailbox password.

This symmetrical encryption happens in the user's web browser using AES-256. Upon the account registration, the user is asked to provide a login password for their account. ProtonMail also offers users to login with two password mode that require a login password and a mailbox password.

- The login password is used for authentication.
- The mailbox password encrypts the user's mailbox that contains received emails, contacts and user information as well as a private encryption key.

Upon logging in, the user has to provide both passwords. This is to access the account and the encrypted mailbox and its private encryption key. The decryption takes place client-side either in a web browser or in one of the apps. The public key and the encrypted private key are both stored on ProtonMail servers. Thus ProtonMail stores decryption keys only in their encrypted form so ProtonMail developers are unable to retrieve user emails nor reset user mailbox passwords. This system absolves ProtonMail from:

- Storing either the unencrypted data or the mailbox password.
- Divulging the contents of past emails but not future emails.
- Decrypting the mailbox if requested or compelled by a court order.

ProtonMail exclusively supports HTTPS and uses TLS with ephemeral key exchange to encrypt all Internet traffic between users and ProtonMail servers. Their 4096-bit RSA SSL certificate is signed by QuoVadis Trustlink Schweiz AG and supports Extended Validation, Certificate Transparency, Public Key Pinning, and Strict Transport Security. Protonmail.com holds an "A+" rating from Ivan Ristic's Qualys SSL Labs.

Several years ago ProtonMail added native support to their web interface and mobile app for Pretty Good Privacy (PGP). This allows a user to export their ProtonMail PGP-encoded public key to others outside of ProtonMail, enabling them to use the key for email encryption. The ProtonMail team plans to support PGP encryption **from** ProtonMail to outside users.

Email sending

An email sent from one ProtonMail account to another is automatically encrypted with the public key of the recipient. Once encrypted, only the private key of the recipient can decrypt the email. When the recipient logs in, their mailbox password decrypts their private key and unlocks their inbox.

Emails sent from ProtonMail to non-ProtonMail email addresses may optionally be sent in plain text or with end-to-end encryption. With encryption, the email is encrypted with AES under a user-supplied password. The recipient receives a link to the ProtonMail website on which they can enter the password and read the decrypted email. ProtonMail assumes that the sender and the recipient have exchanged this password through a back channel. Such emails can be set to self-destruct after a period of time.