(/article/3153445/computers-accessories/40-off-wemo-wi-fi-smart-plug-works-with-amazon-alexa-deal-alert.html)
40% off WeMo Wi-Fi Smart Plug, Works with Amazon Alexa - Deal Alert (/article/3153445/computers-accessories/40-off-wemo-wi-fi-smart-plug-works-with-amazon-alexa-deal-alert.html)

(/article/3181807/wi-fi/31-off-luma-3-piece-whole-home-mesh-wifi-system-deal-alert.html)
31% off Luma 3-Piece Whole Home Mesh WiFi System - Deal Alert (/article/3181807/wi-fi/31-off-luma-3-piece-whole-home-mesh-wifi-system-deal-alert.html)

(/article/3124430/consumer-electronics/63-off-etekcity-3-pack-portable-outdoor-led-camping-lantern-with-9-aa-batteries-deal-alert.html)
75% off Etekcity 4 Pack Portable Outdoor LED Camping Lantern with 12 AA... (/article/3124430/consumer-electronics/63-off-etekcity-3-pack-portable-outdoor-led-camping-lantern-with-9-aa-batteries-deal-alert.html)

LATEST REVIEWS

BitDefender Box

(/article/2910812/bitdefender-box-review-trying-hard-to-be-antivirus-for-the-internet-of-things.html)

Master Lock Co. Bluetooth Smart Keyless Indoor Padlock - 4400

(/article/3036425/connected-home/keyless-padlocks-reviewed-dog-bone-locksmart-bluetooth-vs-master-lock-bluetooth-smart-4400.html)
on Amazon **$45.75 (https://www.amazon.com/Master-Lock-Bluetooth-Padlock-4400D/dp/B01A65T96E%3Fpsc%3D1%26SubscriptionId%3DAKIAIRZJHSP2SKQIWVZA%26tag%3Dpcworld02-20%26linkCode%3Dxm2%26camp%3D2025%26creative%3D165953%26creativeASIN%3DB01A65T96E)**

Dog & Bone LockSmart Bluetooth padlock

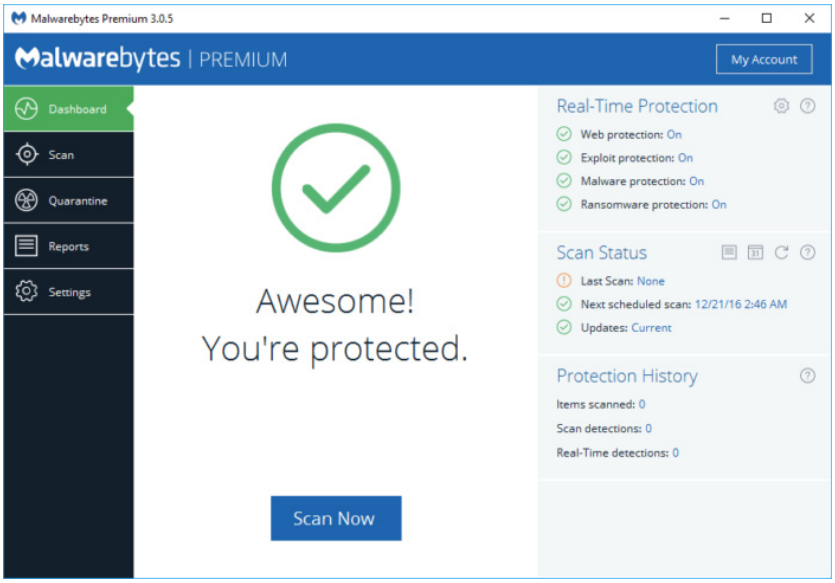
(/article/3036425/connected-home/keyless-padlocks-reviewed-dog-bone-locksmart-bluetooth-vs-master-lock-bluetooth-smart-4400.html)
on Amazon **$49.00 (https://www.amazon.com/Dog-Bone-Locksmart-keyless-bluetooth/dp/B019U0T6TG%3Fpsc%3D1%26SubscriptionId%3DAKIAIRZJHSP2SKQIWVZA%26tag%3Dpcworld02-20%26linkCode%3Dxm2%26camp%3D2025%26creative%3D165953%26creativeASIN%3DB019U0T6TG)**

Ransomware doesn't sneak into your PC like ordinary malware. It bursts in, points a gun at your data, and screams for cash—or else. And if you don't learn to defend yourself, it could happen again and again.

Armed gangs of digital thieves roaming the information superhighway sounds like an overwrought action movie, but the numbers say it's true: Ransomware attacks rose from 3.8 million in 2015 to 638 million in 2016, an increase of *167 times* year over year, according to Sonicwall (http://www.cio.com/article/3166450/security/ransomware-soars-in-2016-while-malware-declines.html)—even as the number of malware attacks declined. Why steal data when you can simply demand cash?

For the first time ever, the RSA security conference in San Francisco held a comprehensive one-day seminar on ransomware, detailing who's being attacked, how much they're taking—and, more importantly, how to block, remove and even negotiate with the crooks holding your data hostage. We came away with a trove of information that you can use to formulate an anti-ransomware strategy.

[Further reading: How the new age of antivirus software will protect your PC] (http://www.pcworld.com/article/3120445/security/how-the-new-age-of-antivirus-softwate-will-protect-your-pc.html)



(https://cms-images.idgesg.net/images/article/2017/01/tech_dangers_for_novices_malwarebytes-100703014-orig.jpg)

Eric Geier

Anti-ransomware solutions like Malwarebytes are a reliable go-to for extra protection from unsavory software, but they're not foolproof.

Ransomware hits you where it hurts—so prepare

Three years ago, my wife's computer was invaded by ransomware, imperiling baby photos, tax documents, and other personal data. My heart sank: Would we have to pay out hundreds of dollars to avoid losing our entire digital lives? Thank goodness, no—because we had already taken most of the steps that the experts recommend.

The first step: Understand your enemy. According to Raj Samani, the chief technology officer of Intel Security's EMEA business, there are over 400 families of ransomware in the wild—even some for Mac OS and Linux (http://www.pcworld.com/article/3041001/security/five-things-you-need-to-know-about-ransomware.html). A survey by Datto found that CryptoLocker (http://www.computerworld.com/article/2485214/microsoft-windows/cryptolocker-how-to-avoid-getting-infected-and-what-to-do-if-you-are.html), which hunts down and imprisons your personal documents via time-locked encryption, was by far the most prevalent. But they vary. One took over a victim's webcam and caught embarrassing footage, threatening to post it online, according to Jeremiah Grossman, chief of security strategy at SentinelOne.

A few common-sense habits can help mitigate your exposure to malware and ransomware, experts say:

- Keep your PC up to date via Windows Update.
- Ensure you have an active firewall and antimalware solution in place. Windows Firewall and Windows Defender are barely adequate, and a good third-party antimalware solution is far better.
- Don't rely on antimalware to save you, however. Experts speaking at the RSA session reminded attendees that antivirus companies were only just getting around to addressing ransomware, and their protection isn't guaranteed.

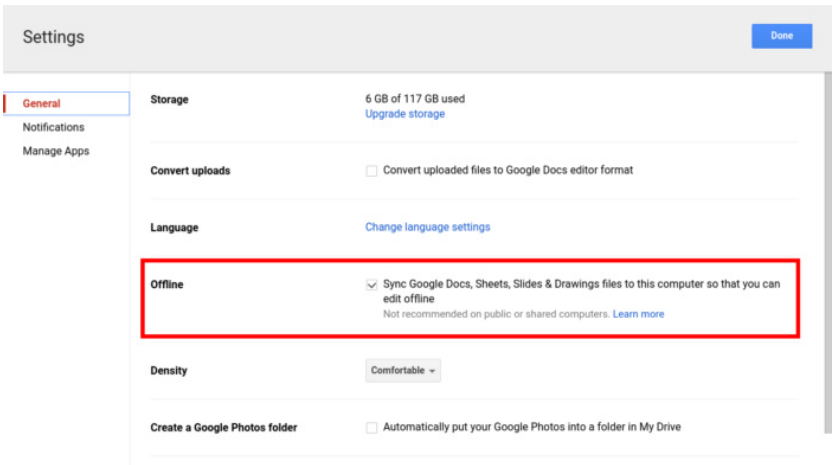
- Ensure that Adobe Flash is turned off, or surf with a browser, like Google Chrome, that turns it off by default.
- Turn off Office macros, if they're enabled. (In Office 2016, you can ensure they're off from the *Trust Center* > *Macro Settings*, or just type "macros" in the search box at the top, then open the "Security" box.)
- Don't open questionable links, either on a webpage or especially in an email. The most common way you'll encounter ransomware is by clicking on a bad link. Worse still, about two-thirds of the infections that Datto tracked were on more than one machine, implying that infected users forwarded the link and exposed more people.
- Likewise, stay out of the bad corners (http://www.pcworld.com/article/2096803/how-to-protect-your-pc-in-the-webs-worst-neighborhoods.html) of the Internet. A bad ad on a legitimate site can still inject malware if you're not careful, but the risks increase if you're surfing where you shouldn't.

For dedicated antimalware protection, consider Malwarebytes 3.0 (https://www.malwarebytes.com/premium/), which is advertised as being capable of fighting ransomware. RansomFree (http://www.pcworld.com/article/3150748/security/this-free-software-protects-your-pc-against-ransomware.html) has also developed what it calls anti-ransomware protection. Typically, however, antimalware programs reserve anti-ransomware for their paid commercial suites. You can download free anti-ransomware protection like Bitdefender's Anti-Ransomware Tool (/cms/article/%20https:/www.bitdefender.com/solutions/anti-ransomware-tool.html), but you're protected from only four common variants of ransomware.

A good, but not perfect, defense: Backup

Ransomware encrypts and locks up the files that are most precious to you—so there's no reason to leave them vulnerable. Backing them up is a good strategy.

Take advantage of the free storage provided by Box, OneDrive, Google Drive, and others, and back up your data frequently. (But beware—your cloud service may back up infected files if you don't act quickly enough.) Better yet, invest in an external hard drive—a Seagate 1TB external hard drive (//buy.geni.us/Proxy.ashx?TSID=14154&GR_URL=https%3A%2F%2Fwww.amazon.com%2FSeagate-Expansion-Portable-External-STEA1000400%2Fdp%2FB00TKFEEAS%253Fpsc%253D1%2526SubscriptionId%253DAKIAIRZJHSP2SKQIWVZA%2526tag%253Dpcworld0220%2526linkCode%253Dxm2%2526camp%253D2025%2526creative%253D165953%2526creativeASIN%253DB00TKFEEAS) is only $55 or so—to add some less-frequently accessed "cold storage." Perform an incremental backup every so often, **then detach the drive** to isolate that copy of your data. (CIO.com has some additional backup advice (http://www.cio.com/article/3085164/backup-recovery/how-to-prepare-for-and-prevent-ransomware-attacks.html) to help defeat ransomware, as does our earlier story (http://www.pcworld.com/article/3056907/security/how-to-stop-ransomware-backup-can-protect-you-but-only-if-you-do-it-right.html).)



(https://cms-images.idgesg.net/images/article/2017/02/sync-google-drive-offline-100708315-orig.jpg)

Ian Paul/PCWorld

You'll feel a lot better if you have your data backed up online and off.

If you are infected, ransomware may allow you to see exactly which files it's holding hostage via File Explorer. One clue may be ordinary .DOC or .DOCX files with strange extensions attached. Ondrej Vlcek, the chief technical officer of Avast, offered an unintuitive piece of advice: If the ransomware isn't time-locked, and you don't need the files right away, consider leaving them alone. (Work on another PC, though.) It's possible that your antivirus solution may be able to unlock them later as it develops countermeasures.

Backup isn't foolproof, however. For one thing, you may need to research how to back up saved games (http://www.pcworld.com/article/2062426/drag-the-princess-to-another-castle-how-to-back-up-your-pc-game-saves.html) and other files that don't fit neatly into "Documents" or "Photos." Ditto for utilities and other custom apps.

What to do if you're infected by ransomware

How do you know you have ransomware? Trust us, you'll know. Ransomware like the busted Citadel ring (http://www.pcworld.com/article/2040881/microsoft-us-feds-disrupt-citadel-botnet-network.html) "warned" that your PC was associated with child pornography, and the imagery associated with most ransomware is designed to invoke stress and fear.

Don't panic. Your first move should be to contact the authorities, including the police and the FBI's Internet Crime Complaint Center (https://www.ic3.gov/default.aspx). Then ascertain the scope of the problem, by going through your directories and determining which of your user files is infected. (If you do find your documents now have odd extension names, try changing them back—some ransomware uses "fake" encryption, merely changing the file names without actually encrypting them.)

The next step? Identification and removal. If you have a paid antimalware solution, scan your hard drive and try contacting your vendor's tech support and help forums. Another excellent resource is NoMoreRansom.com's Crypto-Sheriff (https://www.nomoreransom.org/crypto-sheriff.php), a collection of resources and ransomware uninstallers from Intel, Interpol, and Kaspersky Lab that can help you identify and begin eradicating the ransomware from your system with free removal tools (https://www.nomoreransom.org/decryption-tools.html).

(https://cms-images.idgesg.net/images/article/2017/02/crypto-sheriff-100708822-orig.jpg) NoMoreRansom.org (https://www.nomoreransom.org/crypto-sheriff.php)

The front page of NoMoreRansom.org's Crypto-Sheriff site includes an easy tool to discover what kind of ransomware may be affecting your PC.

If all else fails

Unfortunately, experts say that the key question—*should we pay up, or risk losing everything?*—is often answered by pulling out one's wallet. If you can't remove the ransomware, you'll be forced to consider how much your data is worth, and how quickly you need it. Datto's 2016 survey showed that 42 percent of those small businesses hit by ransomware (http://www.pcworld.com/article/2901672/how-to-prevent-ransomware-what-one-company-learned-the-hard-way.html) paid up.

(https://cms-images.idgesg.net/images/article/2017/02/tescrypt-100709268-orig.jpg)

From Dec. 2015 until May 2016, Tescrypt was the most common ransomware variant detected by Microsoft.

Keep in mind that there's a *person* on the other end of that piece of malware that's ruining your life. If there's a way to message the ransomware authors, experts recommend that you try it. Don't expect to be able to persuade them to unencrypt your files for free. But as crooked as they are, ransomware writers are businessmen, and you can always try asking for more time or negotiating a lower ransom. If nothing else, Grossman said there's no harm in asking for a so-called "proof of life"—what guarantee can the criminal offer that you'll actually get your data back? (Of the companies that Datto surveyed, about a quarter *didn't* get their data back.)

Remember, though, that the point of the prevention, duplication, and backup steps are to give you options. If you have pristine copies of your data saved elsewhere, all you may need to do is reset your PC (http://www.pcworld.com/article/3088749/windows/windows-10-reinstallation-tip-how-to-reset-your-pc-and-remove-everything.html), reinstall your apps, and restore your data from the backup.

Don't let this happen to you

In my situation, my wife and I discovered that we had already backed up everything important to both a cloud service and an external drive. All we lost was a few hours of our evening, including resetting her PC.

Ransomware can infect your PC in any number of ways: a new app, a Flash-based gaming site, an accidental click on a bad ad. In our case, it was a sharp reminder not to go clicking willy-nilly because a "friend" had recommended some bargain shopping site. We're teaching those same lessons to our kids, too.

Ransomware is an unsettling reminder that people mean you harm, and that misfortune may strike at any time. If you treat your PC as part of your home, however—cleaning, maintaining, and securing it from outside threats—you'll rest easier knowing you've prepared for the worst.

To comment on this article and other PCWorld content, visit our Facebook (https://www.facebook.com/PCWorld/) page or our Twitter (https://twitter.com/pcworld) feed.

Related: Security (/Category/Security)

As PCWorld's senior editor, Mark focuses on Microsoft news and chip technology, among other beats.

Follow (/author/Mark-Hachman/) (https://plus.google.com/+MarkHachman/posts) (https://twitter.com/0/109922076073734754844/posts)