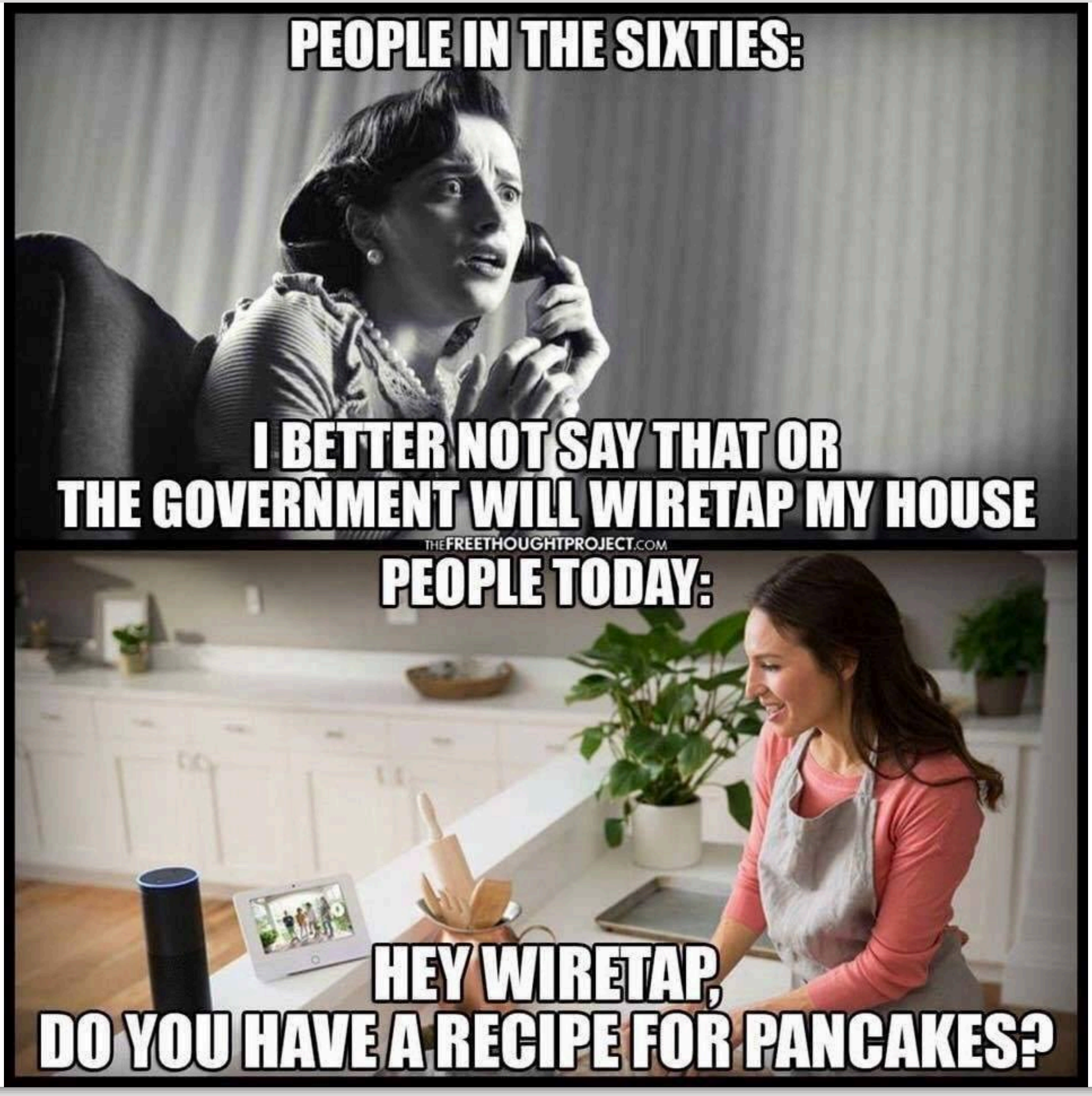
Internet Security:
The IoT (Internet of Things) is Watching You – and Collecting Your Private Data


PEOPLE IN THE SIXTIES:
I BETTER NOT SAY THAT OR
THE GOVERNMENT WILL WIRETAP MY HOUSE
THEFREETHOUGHTPROJECT.COM
PEOPLE TODAY:
HEY WIRETAP,
DO YOU HAVE A RECIPE FOR PANCAKES?

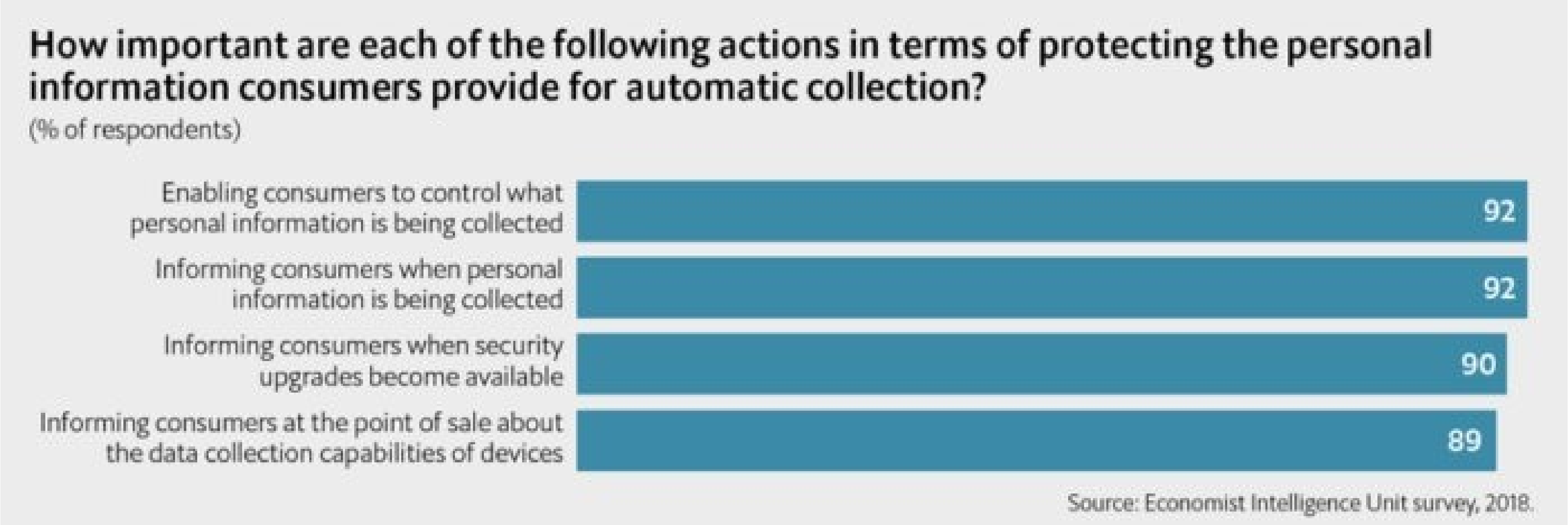
People are really worried about IoT data privacy and security—and they should be

Despite rising spending on IoT security, consumers and businesses are right to worry about how data will be used and protected.

https://www.networkworld.com/article/3267065/people-are-really-worried-about-iot-data-privacy-and-securityand-they-should-be.html

Companies can’t just write off these issues as mere Luddite hysteria over identity theft and consumer behavior profiles. Consumers are unhappy for good reason.

According to a statement from Veronica Lara, who edited the report, “Consumers have cause for concern, as the ubiquity of interconnected sensors through the IoT adds layers of risk that people can’t easily understand. Companies’ lack of transparency and the absence of consumer control over data exacerbate perceptions of privacy and security threats.”



How important are each of the following actions in terms of protecting the personal information consumers provide for automatic collection?

(% of respondents)

Source: Economist Intelligence Unit survey, 2018.

IoT Security: What Are the Ramifications for Spying?

https://www.iotworldtoday.com/2019/02/13/iot-security-what-are-the-ramifications-for-spying

…With the rise of IoT and AI, the amount that Google and other colossal tech companies know about us is poised to expand in ways that are hard to fathom. While adoption is arguably still in the early phases for both, there is little to stop connected sensors from continuing to proliferate all around us while algorithms take charge of a growing list of duties once only performed by humans.

A large number of smartphone users enable tech firms to know nearly each and every location they visit by merely carrying a smartphone with them.

There is already evidence that the connected devices we carry — either near us or even within us — can enable new possibilities for spying. In 2016, former Director of National Intelligence James Clapper said it is possible that the U.S. government would spy on suspects via smart home devices. While that may be more of a possibility than a reality, there are a handful of cases where such devices have enabled unprecedented types of surveillance. One such example comes via a man named Ross Compton who allegedly set fire to his home in 2016 as part of an insurance scam. Local police got a warrant for his pacemaker data and a cardiologist determined that his alibi didn't line up with his cardiac data. He told cops, however, that he broke a window in his house with a cane and threw his possessions out it and then climbed out and pulled heavy items to the front of his house. His steady pulse during the time of the fire apparently told a different story — as did the traces of gasoline outside of his house.

That is an isolated example involving an individual. Consider the possibilities if, say, a nation-state actor or other types of threat actor was able to achieve access to millions of records of citizens — perhaps even collating them with their social security cards and other personally identifiable information….Ultimately, when it comes to cybersecurity, it is hard to make definitive conclusions about broad-based attacks, but it is true that most of us have a growing amount of data being collected about our activities. And, second, that nation-state–based agents appear to be interested in that information.

Data Breaches Increased 54% in 2019 - So Far

https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far
by James Sanders in Security on August 15, 2019, 7:35 AM PST

More than 3,800 data breaches have hit organizations in 2019, according to Risk Based Security.

Despite concerns raised in the cybersecurity community about insider threats, 89% of breaches are the result of outside attacks, though the report notes that "more and more sensitive data is exposed when insiders fail to properly handle or secure the information," pointing to misconfigured databases and services representing 149 of 3,813 incidences reported so far this year resulting in the exposure of over 3.2 billion records.

Risk Based Security also points to the dangers of placing sensitive data in the hands of third parties, naming the American Medical Collection Agency (AMCA) breach, in which "hackers infiltrated AMCA's network and pilfered over 22 million debtors' records including data such as names, addresses, dates of birth, Social Security numbers and financial details" as a critical event. "These breaches be more difficult to manage given the multiple parties involved, they can also have more damaging consequences for the individuals whose data is exposed in the event," the report said, noting that the breach has severe consequences for AMCA, as the company "was forced into filing for bankruptcy protection a mere 2 weeks after news of the breach made headlines."

Healthcare services are the single highest affected industry, according to Risk Based Security, with Retail, Finance/Insurance, Public Administration, and IT rounding out the top five.

For more, check out "Ransomware attacks on businesses up 365% this year"
and "Businesses need to patch for BlueKeep to avoid another WannaCry" on TechRepublic.

IoT Healthcare

https://blog.hubspot.com/marketing/internet-of-things-iot

Outside of the home, IoT is beginning to revolutionize the healthcare and health monitoring industries. Hospitals are already able to remotely monitor their patients' health and collect data using connected medical devices like insulin pumps and heart monitors. This allows doctors to catch early signs of problems and take preventive action.

Within hospitals themselves, connected devices help staff more efficiently manage resources and space. In some cases, that can literally save a life. Sensors on hospital beds that tell when and where beds are open reduce wait times by up to four hours. And monitoring on critical equipment prevents vital hardware from breaking when it is needed most.
Outside of the ER, connected activity trackers like Fitbits enable athletes of all kinds to track their performance and progress. If you're like me and consider walking the quarter of a mile from your car to the office an athletic activity, you can track and log all of those precious steps.

In all seriousness, connected fitness trackers are so helpful even insurance companies are encouraging their customers to wear one. Aetna recently starting giving their employees Apple Watches to keep track of their health and fitness goals, but soon they may be handing them out to all their eligible customers. Why? They hope the watch will encourage users to lead healthier lives, which means fewer insurance claims.

China's hackers are ransacking databases for your health data

New research shows cyber espionage groups linked to China are targeting medical research data and the intellectual property for medical devices.
https://www.wired.co.uk/article/china-hackers-medical-data-cancer

The complicated truth about China's social credit system

China's social credit system isn't a world first but when it's complete it will be unique. The system isn't just as simple as everyone being given a score though.
https://www.wired.co.uk/article/china-social-credit-system-explained

China’s new ‘social credit system’ is a dystopian nightmare

The government claims that its purpose is to enhance trust and social stability by creating a “culture of sincerity” that will “restore social trust.” What it will actually create, of course, is a culture of fear and a nation of informants. This is because one of the ways that people can improve their own social credit score is to report on the supposed misdeeds of others.

Individuals can earn points, for example, for reporting those who violate the new restrictions on religious practice, such as Christians who illegally meet to pray in private homes, or the Muslim Uyghurs and Kazakhs in China’s far west whom they spot praying in public, fasting during Ramadan or just growing a beard. Of course, as the state progresses ever closer toward its goal of monitoring all of the activities of its citizens 24 hours a day, seven days a week, society itself becomes a virtual prison. Western criticism of the new system has been intense, with Human Rights Watch describing it as “chilling.” In response, Chinese Communist Party publications scoff that Westerners are simply too unsophisticated to understand the wonders of the new system.

In the words of China’s Global Times, “The hypothetical theories of the West are based on their ignorance.” The massive social credit system, it goes on to say, is simply “beyond the understanding of Western countries.”
https://nypost.com/2019/05/18/chinas-new-social-credit-system-turns-orwells-1984-into-reality

Data Hacks and Breaches 2019

Data Breaches Increased 54% in 2019 - So Far

by James Sanders in Security on August 15, 2019, 7:35 AM PST

https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far

Everything you wanted to know about data breaches and privacy violations and what to do if you think you've been hacked.

Do you think you've been hacked? Here's what you should do next.
https://www.marketwatch.com/story/100-million-capital-one-customers-were-hacked-everything-you-need-to-know-about-data-breaches-but-are-afraid-to-ask-2019-07-30

If you bought anything from these 19 companies recently, your data may have been stolen

Aug. 15, 2019, 11:20 AM
https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1#panera-bread-19

An Experian poll found that the average consumer uses just five passwords across 26 online accounts.

http://www.theregister.co.uk/2012/07/20/password_reuse_survey

100 million Americans and 6 million Canadians caught up in Capital One breach

Over 1 million Canadian social insurance numbers accessed in breach.

By Chris Duckett | July 29, 2019 -- 23:54 GMT (16:54 PDT) | Topic: Security
https://www.zdnet.com/article/100-million-americans-and-6-million-canadians-caught-up-in-capital-one-breach

Capital One has disclosed that it has suffered a data breach impacting 100 million people in the United States, and 6 million in Canada. The company said in a statement that data between 2005 and 2019 was accessed and related to information on consumers at the time when they applied for a credit card.

"This information included personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income," the company said. "Beyond the credit card application data, the individual also obtained portions of credit card customer data, including: Customer status data, e.g., credit scores, credit limits, balances, payment history, contact information; Fragments of transaction data from a total of 23 days during 2016, 2017 and 2018."

"No bank account numbers or Social Security numbers were compromised," the bank said before listing the above numbers.

It added the configuration vulnerability was disclosed to it by an external security researcher, which led to an internal investigation and discovery of the incident. Although Capital One said its data was encrypted, the attacker was able to decrypt it.

In a separate announcement, the US Attorney's Office for the Western District of Washington said it had arrested a "former Seattle technology company software engineer" in relation to the breach. The accused suspect, Paige Thompson who uses the handle ‘erratic’, appeared in US District Court on Monday and is pending a hearing on August 1.
Thompson is posted on GitHub [publicly available website] the consumer info from the incident,
with the Attorney's Office saying her access was due to a misconfigured web application firewall.

Recent Internet Security News Items – August 2019

Uh-oh: Silicon Valley is building a Chinese-style social credit system

In China, scoring citizens' behavior is official government policy.
U.S. companies are increasingly doing something similar, outside the law.
https://www.fastcompany.com/90394048/uh-oh-silicon-valley-is-building-a-chinese-style-social-credit-system

IoT Report: How Internet of Things technology growth is reaching mainstream companies and consumers

The Internet of Things (IoT) is powering transformation for enterprises, consumers, and governments. Emerging tools and technologies like smart speakers, machine learning, and 5G are enabling huge gains to efficiency and more control at home and in the workplace.
https://www.businessinsider.com/internet-of-things-report

The New Ways Your Boss Is Spying on You

It's not just email. Employers are mining the data their workers generate to figure out what they're up to, and with whom. There's almost nothing you can do about it.
https://www.wsj.com/articles/the-new-ways-your-boss-is-spying-on-you-11563528604

A Huge Ransomware Attack Messes With Texas

Early on August 16, 2019 - a total of 23 local government organizations in Texas were hit by a coordinated ransomware attack. The type of ransomware has not been revealed, and Texas officials asserted that no state networks were compromised in the attack.
https://www.wired.com/story/ransomware-strike-local-texas-government-agencies

MASTERMIND CON MAN BEHIND ‘CATCH ME IF YOU CAN’ TALKS CYBERSECURITY

FAMOUS CON MAN FRANK ABAGNALE: CRIME IS 4,000 TIMES EASIER TODAY

https://creatives.techrepublic.com/whitepapers/TR_Abagnale_Series_Download_r3__1_.pdf

TechRepublic’s Karen Roby sat down with Frank Abagnale (the famous con man turned FBI Academy instructor, who inspired the Leonardo DeCaprio character in the movie ‘Catch Me if You Can’) - to discuss his work at the FBI’s law enforcement training and research center. See what C-suite executives need to know regarding cybersecurity.

PROTECT Yourself and Your Data

At Work

How To Keep Your Private Life Mostly Private at Work

What should you do if you want to keep your personal data private in the workplace? Here are some tips from privacy experts.

Maintain separate devices: Only use your employer-issued phone and laptop for work and keep a separate phone and computer for personal use.

Avoid linking your personal devices to corporate Wi-Fi networks: "Companies routinely log network activity to protect business interests, and most policies make clear there is no expectation of privacy of company equipment," said Marc Rotenberg, executive director of the Washington, D.C.-based nonprofit Electronic Privacy Information Center.

Be careful what you share on your resume: Privacy consultant Michael Bazzell tells clients to anticipate that every piece of personal information shared during the recruitment process could become public through a data breach. He recommends using a Google Voice or internet-based calling phone number rather than your cellphone number, and a commercial mail receiving address like a UPS store.

Use a USB data-blocker: These devices look like thumb drives and sit between a smartphone and a charging cord or dock. They protect smartphone data from being transferred to public charging stations, rental cars or company-owned computers.

Avoid leaking information: Don't publish information about your personal life on public social media accounts like Facebook and Twitter profiles, which can be mined for potentially damaging information by your employer or a company where you have applied for a job.

PROTECT Yourself and Your Data

At Home

https://www.consumer.ftc.gov/topics/privacy-identity-online-security

https://www.consumer.ftc.gov/topics/online-security

Brave Browser

https://brave.com

Brave is built by a team of privacy focused, performance-oriented pioneers of the web, including the inventor of JavaScript and co-founder of Mozilla.

Load pages 2x faster on desktop and up to 8x faster on mobile.

https://brave.com/features

Watch Brave in action, head-to-head-to-head against Chrome and Firefox. Brave loads pages twice as fast out of the box with nothing to install, learn or manage.

Experience unparalleled privacy and security.

Brave fights malware and prevents tracking, keeping your information safe and secure. It's our top priority.

We're not in the personal data business.

Our servers neither see nor store your browsing data – it stays private, on your devices, until you delete it. Which means we won't ever sell your data to third parties.

Defaults that matter

Browse confidently with default settings that block phishing, malware, and malvertising. Also, plugins, which have proven to be a security risk, are disabled by default.

DuckDuckGo

https://duckduckgo.com

Welcome to DuckDuckGo Internet Search

We’re setting the new standard of trust online, empowering people to take control of their information.

You deserve privacy. Companies are **making money** off of **your private information** online without your consent.

At *DuckDuckGo*, we don’t think the Internet should feel so **creepy** and
getting the privacy you deserve online should be as **simple** as closing the blinds.

Our Mission

Too many people believe that you simply can't expect privacy on the Internet. We disagree and have made it our mission to set a new standard of trust online

It's time to take back your privacy!

About Passwords

A strong password has:

- at least 15 characters (preferably random)
- uppercase letters
- lowercase letters
- numbers
- symbols, such as: ` ! " ? $? % ^ & * ( ) _ - + = { [}] : ; @ ' ~ # | \ < , > . ? /

Create Strong Passwords

1Password - https://1password.com Password Manager
LastPass - https://www.lastpass.com Password Manager

Tips for creating strong passwords
A strong password is one that's easy for you to remember but difficult for others to guess. Let's take a look at some of the most important things to consider when creating a password.

Never use personal information such as your name, birthday, user name, or email address. This type of information is often publicly available, which makes it easier for someone to guess your password.

Use a longer password. Your password should be **at least 15 characters long.** Include **numbers, symbols**, and both **uppercase** and **lowercase letters**.

Don't use the same password for each account. If someone discovers your password for one account, all of your other accounts will be vulnerable.

Avoid using words that can be **found in the dictionary**. For example, **swimming1** would be a weak password.

Random passwords are the strongest. If you're having trouble creating one, you can use a password generator instead.

WordPress Website
Wordfence Firewall Blocking Report

This chart represents 7 days of attempted hacking and website access from Blocked countries.

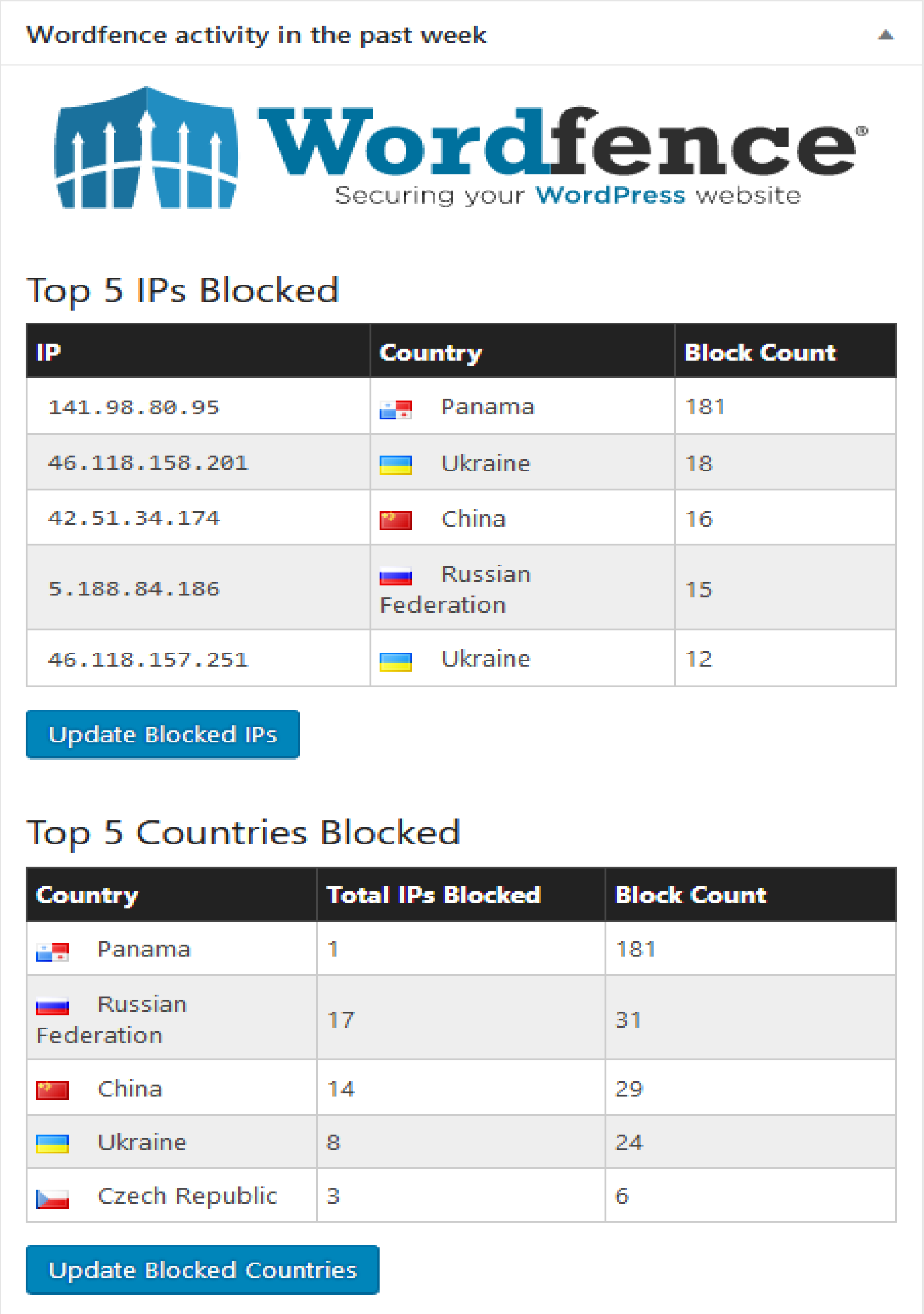
Wordfence Premium is a plugin for WordPress websites. Cost: $99/year.

Wordfence includes an endpoint firewall and malware scanner that were built from the ground up to protect WordPress.

The Threat Defense Feed arms Wordfence with the newest firewall rules, malware signatures and malicious IP addresses it needs to keep your website safe.

Rounded out by a suite of additional features, Wordfence is the most comprehensive security option available.

https://www.wordfence.com



Wordfence activity in the past week

Top 5 IPs Blocked

IP	Country	Block Count
141.98.80.95	Panama	181
46.118.158.201	Ukraine	18
42.51.34.174	China	16
5.188.84.186	Russian Federation	15
46.118.157.251	Ukraine	12

Update Blocked IPs

Top 5 Countries Blocked

Country	Total IPs Blocked	Block Count
Panama	1	181
Russian Federation	17	31
China	14	29
Ukraine	8	24
Czech Republic	3	6

Update Blocked Countries

10,001 Things Hackers Do with Hacked WordPress Websites

In 2016, we cleaned a hacked WordPress business website that had over 10,000 links inserted into the website via the MySQL database.

▪ The page links inserted were not visible from the front of the website.

▪ The website owner had no idea the links were there – until Google banned the website from Search.
(Note: If the website owner had joined Google Webmaster Tools – they would have received notification.)

▪ All 10,000+ links were selling various forms of illegal merchandise; including child porn.

▪ Joining Google Webmaster Tools is FREE – we enroll our clients as a part of our website development services.)

» *With no* regular website maintenance and upkeep of security –
your WordPress website is a hacking magnet.
With proper security and maintenance of your WordPress website – hackers can be stopped.

Preventing Site Hacks – Keeping Your WordPress Site Secure and Maintained!

✓ WordPress CMS critical and regular upgrades, plugin software updates and upgrades, as available.

Per year, WordPress has 4-5 Critical Core Security Updates, Multiple Regular Updates, 100+ plugin updates.

✓ Discontinued plugins are removed. New plugins will be added, when available, at the discretion of **DFW Business Websites**. This happens several times in an average year.

For example: A new and upgraded version of social media share buttons, slideshow or other plugin.

✓ Sometimes a WordPress software upgrade, plugin software upgrade or update can negatively impact site performance. These issues are corrected as a part of the WordPress Website Maintenance Program.

✓ Site back-up and backup archive after each maintenance.

✓ 24/7 Continuous Security Monitoring

Looking forward to growing and securing *your* business online!

DFW BUSINESS WEBSITES
Digital Marketing, SEO, Websites

https://dfwbusinesswebsites.com

469-438-8207

MADE IN TEXAS