THE ASHLEY MADISON DATA LEAK

Back, Evan. "The promise of security, anonymity and safety was just something we said. It wasn't something we did." The Guardian

ABSTRACT

In 2015, the Ashley Madison data breach exposed the private details of millions of users, unleashing a storm of personal, social, and legal repercussions. What began as a targeted cyberattack soon escalated into a global scandal, dismantling relationships, tarnishing reputations, sparking debates on cybersecurity, and personal accountability. This report examines the breach's impact, delves into the

ethical challenges it presented, and explores the critical lessons learned about data protection in the digital age.

Rada, Kayla
Application Security

Contents

Introduction: The Allure of Ashley Madison

In 2015, a website built on the promise of discretion unraveled in one of the most infamous data breaches in history. Ashley Madison—a platform designed to cater to individuals seeking extramarital affairs or those entertaining advances from others—marketed itself as a safe haven for secrecy. Users trusted the site to protect their darkest desires and confidential meetups, believing their privacy was impenetrable.

That illusion was shattered when a hacker group infiltrated Ashley Madison's systems and accessed all its sensitive user data. Targeting its parent company, Avid Life Media, along with sister sites Ashley Madison and Established Men, the hackers issued a chilling ultimatum: delete all user data and shut down the platforms permanently or face the public release of every user's private information. The company's refusal to comply set off a chain of events that devastated lives on a global scale.

The fallout was immediate and catastrophic. Personal secrets were exposed, marriages were destroyed, and careers were ruined. The breach wasn't just a technical failure, it was a breach of trust on a not yet seen level, revealing the vulnerabilities of a platform that had profited from the promise of confidentiality. For some, the consequences proved fatal, with reports of users taking their own lives under the weight of public shame and broken relationships.

What began as a targeted cyberattack quickly became a cultural pivot, raising questions about privacy, ethics, and the consequences of monetizing off the deception. This is the story of how a single breach changed not only lives but also how we perceive the thin boundaries between secrecy and exposure in the digital age.

Let's put yourself in the user's shoes for a moment. Would you hope for the site's closure, knowing that in an industry as profitable as this, another company would surely rise to take its place? The sex industry sells, and if there's demand, someone will supply. Or, on the other hand, would you feel a sense of vindication that your suspicions about a partner's involvement on the site might finally explain those untraceable expenses or suspicious behaviors? And then, there is the possibility of devastation so profound that some might even consider ending their lives, the weight of secrets, guilt, and the potential loss of family ties, pushing some users to consider tragic actions.

Darren Morgenstern's Vison and the Early Years

Ashley Madison was founded in 2001 by Darren Morgenstern in Toronto, Canada, driven by a unique vision to serve a growing, yet largely ignored, demographic. Morgenstern was drawing off data around the 2000s that suggested up to 30% of users on conventional dating sites were already married or in relationships; he sought to create a platform where people could act on their desires without facing judgment. He named the site after two popular female names, "Ashley" and "Madison," according to the founder's brother. Ashley Madison also launched the "Entertainment Males" (EM) service, a feature targeting woman who were looking for male companions. This was a part of the site's larger business strategy to balance gender equality by appealing to female users.

Darren founded the website with the bold tagline *"Life is short. Have an affair,"* reflecting the philosophy that drove its marketing strategy. Morgenstern even claimed that "*80 % of men and 50% of women will cheat on their spouses at some point. It's ingrained in our DNA, and it's not going to change anytime soon"* (Mississauga.com, 2016). This tapped into a cultural shift in the early 2000s, where people were becoming more comfortable with digital ways to explore dating and desires. The site's early success was fueled by this bold approach and *"underserved"* market, particularly targeting men seeking affairs with women who were, according to the site, just as eager for extramarital meetups. In 2007, just six years after its founding, Darren sold Ashley Madison to Avid Life Media.

In the beginning, Ashley Madison's business model was straightforward yet highly effective: women could join the platform for free, making it enticing to the male users who needed more motivation to sign up. Since women were statistically less likely to seek affairs, the business model aimed to make it as easy as possible for these women to sign up, regardless of their relationship status. On the other hand, men were required to pay to access the sites' features. The credit purchasing system was based on what Ashley Madison called a “token-based” credit system rather than the straightforward subscription system we see today. For example, men would spend 5–10 credits (roughly $5) just to send a message. That didn’t include the more expensive features like sending “virtual gifts” or using “priority mail” which further increased the males spending.

Ashley Madison’s credit system followed this pricing model:

- 100 credits for approximately $50
- 500 credits for $150
- 1,000 credits for $250

Those more expensive features were designed to increase user engagement: the “Traveling Man” feature, which allowed users to connect with people in other locations; the “Priority Mail” system, which gave a message a priority placement in the receiver’s inbox; the “Virtual Gifts,” which were just intangible virtual items to rack up more profits for the business.

However, one of the more controversial aspects of the site was its “Full Delete” feature, which promised users that for a fee of $19 USD to fully delete their profile. This service was marketed as a way for users to ensure their privacy, though this feature played a part in Ashley Madison’s appeal, its effectiveness would come into question later. The details of how this paid service failed to live up to its promise.

The Rise: Noel Biderman

Ashley Madison was slow to gain traction when it first launched. Exact numbers on the site's early user base are difficult to pinpoint, but estimates suggest that only a few hundred thousand people had been signed up before the site was sold to Avid Life Media in 2007. However, a pivotal shift occurred that transformed the company's slow-burn trajectory, largely thanks to one man: Noel Biderman. Biderman was brought in as the CEO and teamed up with his childhood best friend Evan Back as Vice President. Together, the two introduced an aggressive marketing strategy that the site would soon feel.

Under Biderman, the platform adopted a bold and unapologetic approach to advertising. They used bold statements and alluring messages to attract their target audiences. However, when major networks began rejecting their provocative ads, Biderman and Back found alternative ways around these rejections by deciding to market to U.S. audiences by targeting cable networks or digital platforms that allowed more leeway in terms of what could be said and shown. Their tagline, "Life is short. Have an affair" or "Your wife doesn't need to know" pushing the idea of secrecy and discreet connections. These ads played into the niche nature of the site and were working to evoke curiosity or even outrage, making them memorable.

The outrage was growing quickly with very public ads and wild statements created by Ashley Madison's team that Biderman was quick to defend the business. He argues that the site wasn't responsible for creating cheaters but was merely meeting an existing need within society. In an interview with The Globe and Mail in 2014, he explained: *"Were not creating anything that isn't already out there. We're simply providing a platform for those who already have a desire to cheat and were doing so in a safe and discrete manner."*

By 2015, Ashley Madison had skyrocketed to over 37 million users and was widely used in more than 40 countries. This growth was largely attributed to Biderman's leadership and the company's willingness to use unconventional tactics. However, as the platform became more prominent, so did the scrutiny around the business model, ethical implications, and privacy of its users. This would eventually culminate in a major crisis for the company in 2015, when a hacker group exposed millions of users' information, setting the stage that would permanently tarnish the brand's image.

Day One: The Calm Before the Storm

On the morning of July 19, 2015, approximately 200-250 employees at Ashley Madison's Toronto headquarters arrived for what they thought would be a typical day at the office. However, things quickly took a turn as they walked to their respective desks. They were told not to touch their computers - not like there was an option, as every computer in the facility was greeted by a chilling message from a hacker group calling themselves The Impact Team. The ominous message read: "AM AND EM MUST SHUT DOWN IMMEDIATELY PERMANENTLY. We are the Impact Team, we have taken over all systems in your entire office and production domains, all customer information databases, source code repositories, financial records, and emails. Shutting down AM and EM will cost you, but non-compliance will cost you more; We will release all customer records, profiles with all the customers' secret sexual fantasies, nude pictures, conversations and matching credit card transactions, real names and addresses, and employee documents and emails. Avid Life Media will be liable for fraud and extreme harm to millions of users." The hackers didn't just expose vulnerabilities in the company's systems but were highlighting its moral contradictions, accusing it of fraud and causing harm to millions of users. It was clear that the attack wasn't about financial gain; it was a moral outrage.

The atmosphere at the office quickly became tense and chaotic; employees were instructed not to touch their computers, leaving many confused and anxious. For some, there was a sense of disbelief that such a targeted attack could occur. Others worried about what this breach meant for their personal security, as the hackers also threatened to release internal employee details. At first, Ashley Madison's leadership treated the hacker's threat as little more than a bluff. With no explicit ransom or further communication from The Impact Team, the company assumed it might be a scare tactic rather than a genuine breach.

To address the issue, CEO Noel Biderman brought in top-tier cybersecurity experts to investigate. Their goal was to assess the extent of the intrusion and determine whether any data had been compromised. However, the lack of urgency in the company's approach may have stemmed from a desire to downplay the incident, particularly with an Initial Public Offering (IPO) on the horizon.

Human Error: Biderman's Ego

Ashley Madison's marketing was built on a foundation of discretion and "trust"—ironic given the site's purpose. It promised anonymity and privacy, allowing users to explore secret desires without fear of exposure. Transactions for Ashley Masion services were deliberately obscured on credit card statements, appearing under unrelated business names to prevent suspicion. The customer service team was trained to deflect calls from suspicious spouses, advising them to dispute charges with their credit card companies. The entire operation was a well-oiled machine designed to help users hide in plain sight. (Paton, 2024)

CEO Noel Biderman took this narrative to a personal level. Known for his brash confidence, he publicly defended the site every chance he got. In interviews, Biderman often presented himself alongside his wife, who vouched for his personal faithfulness, framing their relationship as proof the platform was not a cause of infidelity. However, this confidence ultimately became his downfall. This air of confidence would ultimately prove to be a liability. By projecting himself as a symbol of trustworthiness and loyalty, Biderman made the company's promises of privacy and discretion feel genuine. And yet, when the Impact Team's threat finally came to a head, Biderman's confidence would be revealed as a fraud, and the site's promises would fall apart in the most public way possible.

The IPO was pivotal to Ashley Madison's strategy to gain legitimacy. Biderman envisioned it as an opportunity to reframe the company's reputation. By going public, AM sought to shed some of its reputation off but present itself as a legitimate business that is just addressing a “market need.” The IPO could have provided the financial muscle to grow and improve its technology infrastructure. For Biderman and other insiders, this could have represented a financial return. If the IPO went through, it could have been seen as a double-edged sword, a chance for growth, but also it would have spotlighted its vulnerabilities. In the end, the hack not only derailed these ambitions but also highlighted the risks Biderman was willing to take to legitimize Ashley Madison.

The 30-Day Ultimatum

On July 19th, 2015, a reporter named Brain Krebs broke the story, revealing that a group of hackers, known as The Impact Team, has collected around 40 MB of sensitive data from Avid Life Media. Shortly after, CEO Noel Biderman speculated that the breach might have been an inside job or by someone who “touched” ALM’s IT system. On July 20th, at 12:25 PM, Avid Life Media made a public statement saying they were aware of an attempt to gain access to our systems. Saying, “We have always had the confidentiality of our customers information foremost in our minds; we have had stringent security measures in place, including working with leading IT vendors from around the world” (post by media@ashleymadison.com).

I found a second statement released by the Impact Team on a Pastebin post, advising a 30-day window for avid life media to shut down. But the statement goes on to say, “We are the Impact Team. We hacked them completely... over the past few years have taken all customer information databases, complete source code repositories, financial records, documentation, and emails, as we prove here. And it was easy. For a company, whose main promise is secrecy, it’s like you didn’t even try, like you thought you had never pissed anyone off.” Their statement goes on to say that they have instructed ALM to take down Ashley Madison and Established Men permanently. How upset the team is that ALM lied about the “Full Delete” option and how “ALM netted $1.7 million in revenue in 2014” from this feature, and it’s a complete lie. The team did apologize to Mark Steel (Director of Security). “You did everything you could, but nothing you could have done could have stopped this.” Going on they advised this was the last warning, leaving the statement with, “Well, Noel? Trevor? Rizwan? What’s it going to be?”

In the days following the ultimatum, the Impact Team escalated their threats. On July 22, 2015, the group publicly exposed two Ashley Madison users, a man from Brockton, MA, and a man from Ontario, Canada. Exposing their email, address, fantasies, log-in ID, and full password hash. Further demonstrating that they not only had the data but also knew how to analyze it. The group hinted they might continue releasing one user per day until the 30-day window closed or the websites were taken offline.

On August 18th, 2015, Impact Team's 30-day window ultimatum expired, but of course, both Ashley Madison and Established Men are still online. In another Pastebin post titled "TIMES UP!" The team releases the first significant portion of Ashley Madison's user data dump. Using a torrent file containing 10 GB of the users' emails, physical addresses, fantasies, hashed passwords, and credit card information. Avid Life Media released a statement acknowledging the breach, stating they *"were working with authorities to investigate, and claiming the hackers were not "hacktivists" but criminals."* (Wikipedia). In the following days of August 19th-20th "search websites" started popping up that let users search to see if their email addresses were leaked. The first data dump exposed the personal details of millions of users, triggering a media frenzy as individuals and news outlets scoured the lists for recognizable names.

On August 20th, 2015, the Impact Team leaks a second major dump of the AM data. Unlike the first release on the 18th this one contained around 60 GB of the user's data. This dump was mostly internal data, including Avid Life Media CEO Noel Biderman's emails and Ashley Madison's website source code. In total, the hack exposed over 37 million users. The consequences were swift and severe, as the leak led to public shame, intense scrutiny, and unrecoverable damage to reputations. The companies would soon see multiclass action lawsuits, and the company would also offer a $500,000 reward for information on the Impact team or the attack.

The Exposed

Beyond the individual lives shattered by the breach, the data dump revealed deeper issues within Ashley Madison itself. Just a week after the first major dump, reports of blackmail and identity theft were starting to target the leaked Ashley Madison users. On August 28th, 2015, Noel Biderman, whose emails were leaked in the second data dump, stepped down, Avid Life Media released a statement that "it's in the best interest of the company and allows us to continue to provide support to our members and dedicated employees." (prnewswire.com 2015).

One of the most significant revelations was the discrepancy between the advertised number of active female users, which was far lower than advertised. From an article from Gizmodo, *"out of 5.5 million female accounts, roughly zero percent show any kind of activity at all, after the day they were created. "(*Annalee Newitz 2015) This misleading male users by promoting a false narrative: many of the women the male users believed they were chatting with were not real individuals, but bots or even Ashley Madison employees. This revelation was devastating to male users who had been spending large sums of money on tokens to message these supposedly interested women or to access explicit images, only to find out their interactions were manipulated by the company to increase profits.

On September 9th, 2015, researcher Gabor Szathmari announces that he had discovered poor security practices in Ashley Madison's source code. He goes on to say that the database passwords were between 5 and 8 characters, and many of them contained two-character classes only. The company's private keys of SSl certificates are also stored in the repository; API secrets and authentication tokens were so easy to see in 10 minutes. He also noticed that the website didn’t employ form or email validation to screen out the bots. He sheds some light on potential methods that could have been used in the attack. (Gabor, Sept 7th, 2015)

Some of the most high-profile individuals revealed in the breach included the YouTube couple Sam and Nia Rader, who had built their family channel around their love and faith. When Sam’s account on the site was exposed, their channel was banned, and their public image suffered. Reality star Josh Duggar from *19 Kids and Counting* also found himself in the spotlight, eventually issuing a public apology and revealing his personal life struggles after the attack.

Rumors circulated that other prominent individuals, including Hunter Biden and various government officials, were on the list, though some of these claims remain unverified or hidden. The impact went beyond just reputational damage; tragically, some individuals could not withstand the fallout. Reports linked two suicides, one of a pastor and another of a professor at the New Orleans Baptist Theological Seminary, to the data leak. Both their families reportedly cited the exposure as a driving factor. Unconfirmed reports mentioned two additional suicides in Toronto, Canada, and one in the United States, underscoring the gravity of the leak’s consequences.

Impact Team

The Ashley Madison hack remains one of the most infamous breaches in cybersecurity history, not just for its scale but for the motivations and methods of the hackers, known as the Impact Team. Their statement set the tone early on:

> "*We are not opportunistic skids with DDoS or SQLi scanners or defacements. We are dedicated, focused, skilled, and were never going away. If you profit off the pain of others, whatever it takes, we will completely own you."*

From the start it was clear this was more than a typical data heist; it was a calculated and deeply personal attack targeting the company's practices and leadership.

So, why Ashley Madison? The Impact Team hadn't hacked before and hasn't been active since. They claimed ethical motivations, criticizing Avid Life Media's (ALM) deceptive practices. But security experts were divided on their true intentions. Some, Like Robert Graham of Errata Security, suggested it was about the thrill: *"They appear to be motivated by the immorality of adultery, but in all probability, their motivation is that #1 it's fun and #2 because they can,"* (Robert Graham, 2015) Others, like Norwegian researcher Per Thorsheim, pointed to timing, noting that ALM had been moving toward an IPO just before the hack. *"It's not just for the fun and 'because we can,' nor is it just what I would call 'moralistic fundamentalism."*

"Given that the company had been moving toward an IPO right before the hack went public, the timing of the data leaks was likely no coincidence." (Thorsheim 2015).

In an interview between The Impact Team and with Joseph Cox on Vice.com on August 21st, 2015, the team only agreed to answer questions via email. Q&A below.

- How did you hack Avid Life Media? Was it hard?
  The Impact Team: "*We worked hard to make fully undetectable attack, then got in and found nothing to bypass."*
- What was their security like?
  "Bad. Nobody was watching. No security. Only thing was segmented network. You could use Pass1234 from the internet to VPN to root on all servers."
- When did you start hacking them? Years ago?
  "A long time ago."
- What were your motivations for the hack?
  "We were in Avid Life Media a long time to understand and get everything. Finally we watched Ashley Madison signups growing and human trafficking on the sites. Everyone is saying 37 million! Blackmail users! We didn't blackmail users. Avid Life Media blackmailed them. But any hacking team could have. We did it to stop the next 60 million. Avid Life Media is like a drug dealer abusing addicts."
- How experienced are the hackers in The Impact Team?
  "Very."
- Will The Impact Team be hacking any other sites in the future? If so, what targets or sort of targets do you have in mind?
  "Not just sites. Any companies that make 100s of millions profiting off pain of others, secrets, and lies. Maybe corrupt politicians. If we do, it will be a long time, but it will be total."

In 2014, ALM reported revenues of $115 million, a figure that made one thing clear, the company was never going to bow to demands or shut down. For the Impact Team, this was never about negotiation, it was about making a statement and letting the fallout unfold. Unlike the typical cyberattacks that might rely on DDoS disruptions or quick scans for weak points, the Impact Team took a much more calculated and sophisticated approach. Their goal wasn't financial gain; it was to shine a spotlight on Ashley Madisons's deceptive practices, highlighting privacy breaches and ethical misconduct that lurked beneath the surface. This wasn't just about exposing user data, it was direct challenge to the company's leadership, with CEO Noel Biderman front and center (and possibly others like Trevor or Rizwan, based on their involvement) Their first message, released alongside the hacked data, summed it up in two words: "Times Up." It marked the end of Ashley Madisons promises and anonymity and trust.

Theories on How They Were Hacked

The methods used by the Impact Team to hack Ashley Madison remain unclear, but several theories have surfaced:

1. SQL Injection: This is considered one of the most likely culprits. One user theorized that Ashley Madison's subdomains could have contained a poorly monitored parameter, allowing hackers to exploit it through SQL injection. Another user noted that this approach could have been used to retrieve sensitive data, potentially even stealing verification codes to reset admin account passwords.

2. Weak Passwords and Social Engineering: The thread mentions the possibility that hackers exploited weak corporate passwords, like "Pass1234," to gain access. Some users suggested that social engineering (SE) could have played a role, where an employee might have been manipulated into revealing login details.

3. Spear Phishing and Malware: Another theory points to spear phishing, where targeted emails could have been used to drop malware onto a developer's computer. With malware in place, hackers could navigate the network more freely. A user highlighted that, while this is feasible, it depends on the developer using a specific operating system (e.g., Windows), which introduces variables that complicate the attack.

4. Complex Layered Attack: A theory combines SQL injection with malware deployment. A hacker could have exploited a vulnerable parameter to inject malware into the site, then triggered a chain reaction, such as forcing a developer to troubleshoot the site and unwittingly activating the malware. This scenario, though intricate, was deemed unlikely by some users due to the number of steps and dependencies involved.
5. Insider Help: Some experts believe the attackers might have inside information or assistance. Their detailed understanding of Ashley Madison's internal operations supports this theory.
6. Unpatched Vulnerabilities: Reports following the breach revealed several unpatched vulnerabilities in Ashley Madison's systems, which could have provided easy access for hackers.

The thread also highlights the challenge of balancing technical feasibility with practical simplicity. While SQL injection appears to be the easiest explanation, the extent of the breach—reaching into Windows Domain controls and corporate systems—suggests that multiple vulnerabilities, potentially exploited in tandem, were at play.

Others propose that the breach might have been an inside job, carried out by a disgruntled employee or someone with internal access. Another possibility is spear phishing, where hackers tricked a developer into downloading malware, giving them access to the network.

The Impact Team also mentioned Ashley Madison's poor security culture, pointing to corporate accounts with weak passwords. As one Reddit user put it, "Looks like someone was socially engineered and had a weak password—most of the corporate accounts were laughably bad."

While the exact details remain speculative, these theories underline a combination of technical vulnerabilities and human errors that likely contributed to the hack.

Epilog: Cautionary Lessons

The Ashley Madison hack was a wake-up call for the digital age, showing just how devastating a data breach can be when sensitive user information isn't properly protected. Even though the company has since rebranded as Ruby Corp. and beefed up its security protocols, the breach left a lasting impression on users and businesses, highlighting risks that go far beyond financial losses.

The fallout for the hack was immense. Following the public release of millions of user records, Ashley Madison faced a wave of legal challenges, including a class action lawsuit from the affected users. ALM rebranded to Ruby Corp. in July 2016 in attempts to rebuild its image, also distancing themselves from their controversial slogan, "Life is show, have an affair" shifting to "open-minded relationships" to shed off the site's scandalous reputation. By July of 2017, Ruby Corp. paid out $11.2 million settlement to compensate the victims. Rebuilding trust and improving data security took not just them but another financial investment, and it's a sobering reminder how critical it is to get cybersecurity right from the start.

So, what else went wrong? According to *CynoSure Prime*, a password-cracking group, Ashley Madison didn't prioritize strong encryption methods, leaving over 11 million passwords vulnerable. Many of those passwords were laughably weak, think like "123456", which only made matters worse. On top of that, the company's network lacked the property segmentation and monitoring, giving attackers free rein to explore their systems without being detected for far too long. Beyond the technical flaws, the lack of ethics and transparency stood out. For example, the company charging for a “full delete” feature, claiming it would erase their accounts entirely, but in reality, the data wasn’t being deleted at all. This pushed the industry to prioritize not only technical safeguards but also the moral obligations companies have to their users.

What can we learn from all this? First, companies must adopt comprehensive security measures. There should be transparency about how user data is stored and managed, building trust with users. Encouraging users to adopt strong passwords and multi-factor security measures, that users and staff members alike need to enforce. Ensuring routine security testing with protocols and procedures of the business. Organizations need to educate their staff and users alike on digital safety. Acknowledging the cyber security is a shared responsibility across all organizational levels.

If the Ashley Madison hack happened today, could it be prevented? Thankfully cybersecurity practices have advanced significantly since 2015, and several modern measures could mitigate or even prevent such an attack:

- Stronger Password Policies: Enforcing complex, unique passwords and eliminating defaults like "Pass1234" would have significantly raised the bar for attackers. Modern systems use password managers, combined with tools like password entropy checks, to minimize weak credentials.
- Multifactor Authentication (MFA): MFA could have added an extra layer of security, even if passwords were compromised. Attackers would need access to a second factor, such as a user’s phone or hardware token, to proceed.
- Improved Network Segmentation: Proper segmentation limits the damage of a breach by restricting lateral movement within the network. If ALM had segmented sensitive data from less critical systems, attackers wouldn’t have been able to access everything so easily.
- Real-Time Monitoring and Intrusion Detection: Advanced monitoring tools, such as SIEM (Security Information and Event Management) systems and AI-driven

anomaly detection, can identify suspicious activity quickly and alert administrators before significant damage occurs.

- Zero Trust Architecture: Adopting a Zero Trust model ensures that no user or system is trusted by default, requiring continuous verification of identity and permissions to access data or systems.

For companies, it's clear: cybersecurity isn't just an IT issue, it's a company wide responsibility. And for users, it's a call to take ownership of your online safety. It in a interconnected world, protecting privacy and trust is a shared effort, and the lessons from Ashley Madisons breach will continue to share how we approach digital security.

Cites:

Paton, T. (Director). (2024). *Ashley Madison: Sex, Lies & Scandal* [Documentary series]. Minnow Films. Available on Netflix.

Back, E. (2015). *"The promise of security, anonymity and safety was just something we said. It wasn't something we did." The Guardian*. Retrieved from https://www.theguardian.com/tv-and-radio/article/2024/may/14/ashley-madison-netflix-documentary

"*80 % of men and 50% of women will cheat on their spouses at some point. It's ingrained in out DNA, and it's not going to change anytime soon"* (Mississauga.com, 2016). https://www.mississauga.com/news/ashley-madison-founder-discusses-loyalty-and-good-business/article_44f923fe-b446-586f-bb54-e9d8da23eaa6.html

Reddit User stories from https://www.reddit.com/r/adultery/comments/hwlno4/ashley_madison_the_guide_to_everything_you_did/

“Were not creating anything that isn’t already out there. We’re simply providing a platform for those who already have a desire to cheat and were doing so in a safe and discrete manner.” https://www.theglobeandmail.com/life/relationships/meet-the-man-behind-ashleymadisoncom/article570197/

https://en.wikipedia.org/wiki/Ashley_Madison_data_breach

https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/
https://www.prnewswire.com/news-releases/statement-from-avid-life-media---august-28-2015-300134655.html
*“out of 5.5 million female accounts, roughly zero percent show any kind of activity at all, after the day they were created.”(*Annalee Newitz 2015)
https://gizmodo.com/almost-none-of-the-women-in-the-ashley-madison-database-1725558944
https://blog.gaborszathmari.me/credentials-in-the-ashley-madison-sources/

“They appear to be motivated by the immorality of adultery, but in all probability, their motivation is that #1 it’s fun and #2 because they can,” (Robert Graham, 2015)
https://blog.erratasec.com/2015/08/notes-on-ashley-madison-dump.html#.VdeFVyRiM20

“It’s not just for the fun and ‘because we can,’ nor is it just what I would call ‘moralistic fundamentalism” “Given that the company had been moving toward an IPO right before the hack went public, the timing of the data leaks was likely no coincidence.”
https://www.wired.com/2015/08/ashley-madison-hack-everything-you-need-to-know-your-questions-explained/

https://www.vice.com/en/article/ashley-madison-hackers-speak-out-nobody-was-watching/

Reddit. (2015). Theories on the Ashley Madison hack. Retrieved from https://www.reddit.com/r/hacking/comments/3hkuqn/your_theory_on_how_does_ashley_madison_got/?rdt=44152