Get Secure & Stay Secure: The Unconventional Guide to Mobile App Security

With 6 Examples of High Profile
Security Breaches

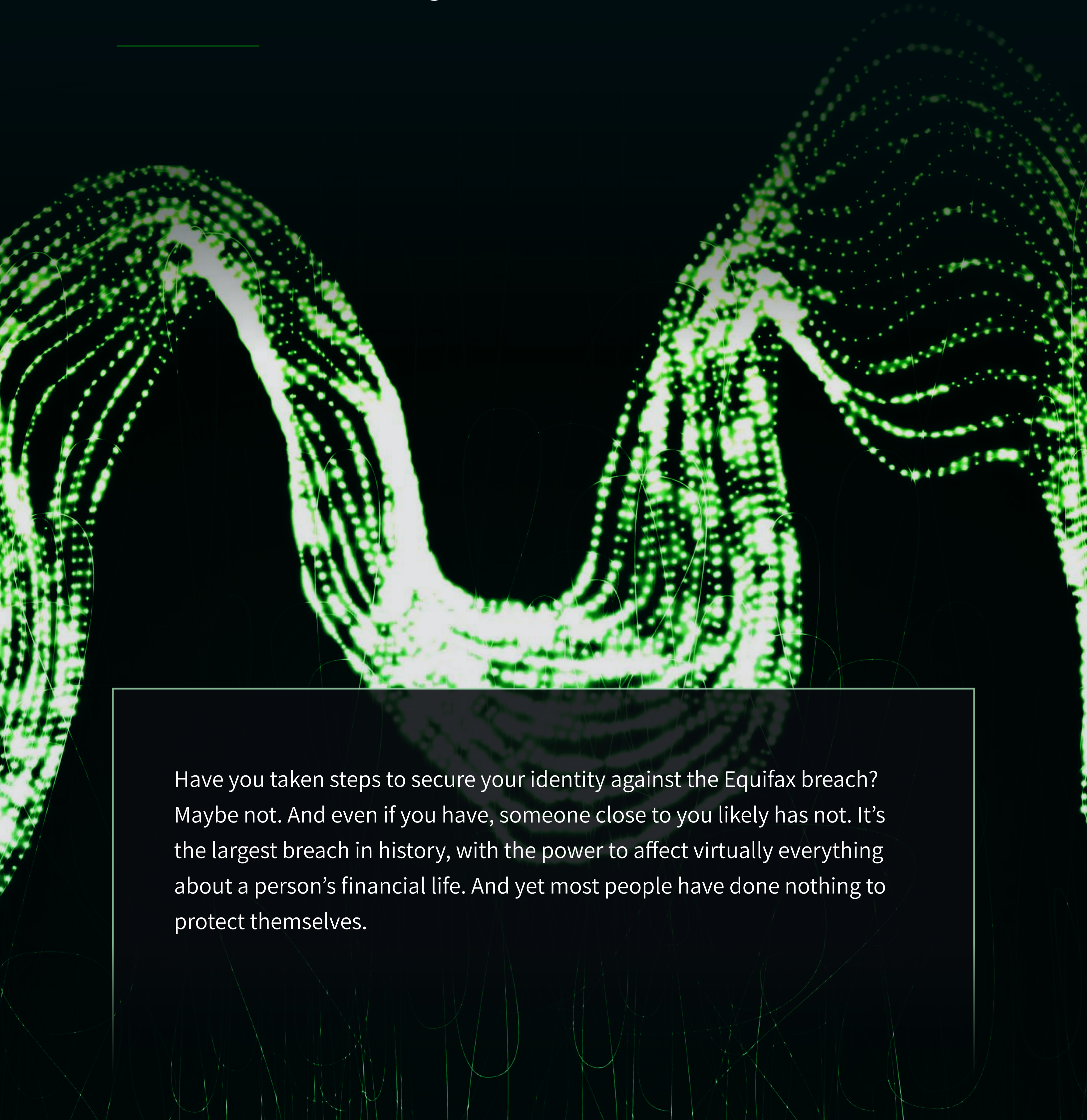
a guide by

APP SOLID.

As consumers and businesses are still reeling from the fallout of the Equifax security breach, app developers across the globe have begun to explore what they can do to avoid becoming the next cautionary tale. Even so, we continue to find that most apps are not properly secured. We know there’s a threat. Developers know there’s a threat. Consumers know there’s a threat. So why is everyone so unconcerned about their own app security?

Here’s what you need to know about the many barriers good app security faces -- and how you can break through those barriers to protect your business and your customers.

‘It Won’t Happen to Me’: The Psychology of App Security



Have you taken steps to secure your identity against the Equifax breach? Maybe not. And even if you have, someone close to you likely has not. It’s the largest breach in history, with the power to affect virtually everything about a person’s financial life. And yet most people have done nothing to protect themselves.

Why is this?

There's a curious psychology at play behind our collective refusal to select good passwords, install security updates, shell out a little extra to protect our identities, and otherwise treat our mobile devices to the same security we treat our homes. Understanding the various factors that play a role in this fallacious thinking is key to implementing sound mobile security.

Here's what we know about the psychology of mobile app security:

No one thinks they'll be a target

Life is stressful enough. No one wants to waste precious time contemplating all the things that could go wrong -- particularly when things already are going wrong. This means that the people most vulnerable to catastrophic consequences following a breach -- those who can't afford to lose money, those who don't know how to dispute charges, those who are too stressed or busy or sick to deal with a major financial hurdle -- are also the least likely to take proactive steps to secure their accounts and devices.

It all feels like too much stress. And even if you can break through that barrier, most people think they're not a valuable target. They think hackers only want to target "rich people." And almost no one sees themselves as rich -- even though virtually everyone has a credit card, a few dollars in the bank, or some resource that a hacker can take advantage of. You don't need a ton of money. You just need a fresh identity, a valuable piece of data, a line of credit, or a bank account. That's all it takes to become a target.

It’s inconvenient to take basic security steps

The most secure passwords are long. They’re also frequently changed. That means they’re hard to remember, and users may need to maintain password logs or cultivate memory tricks.

Double factor authentication is time-consuming, and can be confusing to users who aren’t tech-savvy.

Installing security updates takes time, and sometimes changes the way a device functions.

Are you noticing a trend?

Ultimately, most users don’t take appropriate security measures because it’s inconvenient. We live in a high-stress, exhausting world in which everyone has too much to do and not enough time in which to do it. When security steps are challenging or time-consuming, people are more likely to ignore them.

We don’t see our devices as valuable

Few people would leave their most valuable items near the front door, then leave the front door open and unlocked, with the dog gated far away on the other side of the house. Yet that’s precisely what most people are doing with their devices. They do little to secure them, and much to advertise the valuable information they have. For instance, by installing a financial app, a user advertises to device thieves or hackers that there may be financial information stored on the device.

We’re used to living in an analog world. Adjusting our expectations to view digital information as equally valuable takes time. Until it becomes second nature, it’s up to the tech savvy among us to remind users that their whole lives and entire financial histories may be stored on their digital devices.

We engage in victim-blaming

When we hear about a crime, we look for what the victim did wrong. That way we can avoid the same fate. Robbed at the ATM? You shouldn’t have been there at night. Lost your possessions in a break-in? Your alarm system should have been activated. We engage in the same sort of victim-blaming with digital crimes. We look for ways the victim might have caused their own victimization. They didn’t understand how the Internet works, or they had a bad password, or they left their phone somewhere, or... the list goes on and on. It’s human nature to want to feel safe. And that means finding some way to blame crime victims.

There’s always something that could have been done differently. It usually involves properly securing the device. So rather than looking for esoteric things users did wrong, consumers are better served by noticing the obvious need to secure their digital devices.

We’d rather correct a problem than avoid it in the first place

Even if you can break through these thought errors, most consumers cling to another one. They insist that they’d rather correct the aftermath of a security breach than take proactive steps to prevent one from occurring in the first place. They think they can just freeze their credit, dispute fraudulent charges, and call it a day.

The reality is that it can take months, and even years, to clean up a security mess. Worse still, consumers might not notice they’ve been a target until it’s too late to dispute the charges—or until they’ve lost a massive sum of money and can’t pay their bills. Educating consumers about how much time, effort, and money it takes to clean up the mess a breach leaves behind often encourages them to make better decisions.

Overcoming the Psychological Barriers to App Security

Mobile app security is a technical issue, first and foremost. That’s why AppSolid offers industry-leading binary protection. It works. It’s proven. Half the battle, however, is getting users to understand that their devices are under attack.

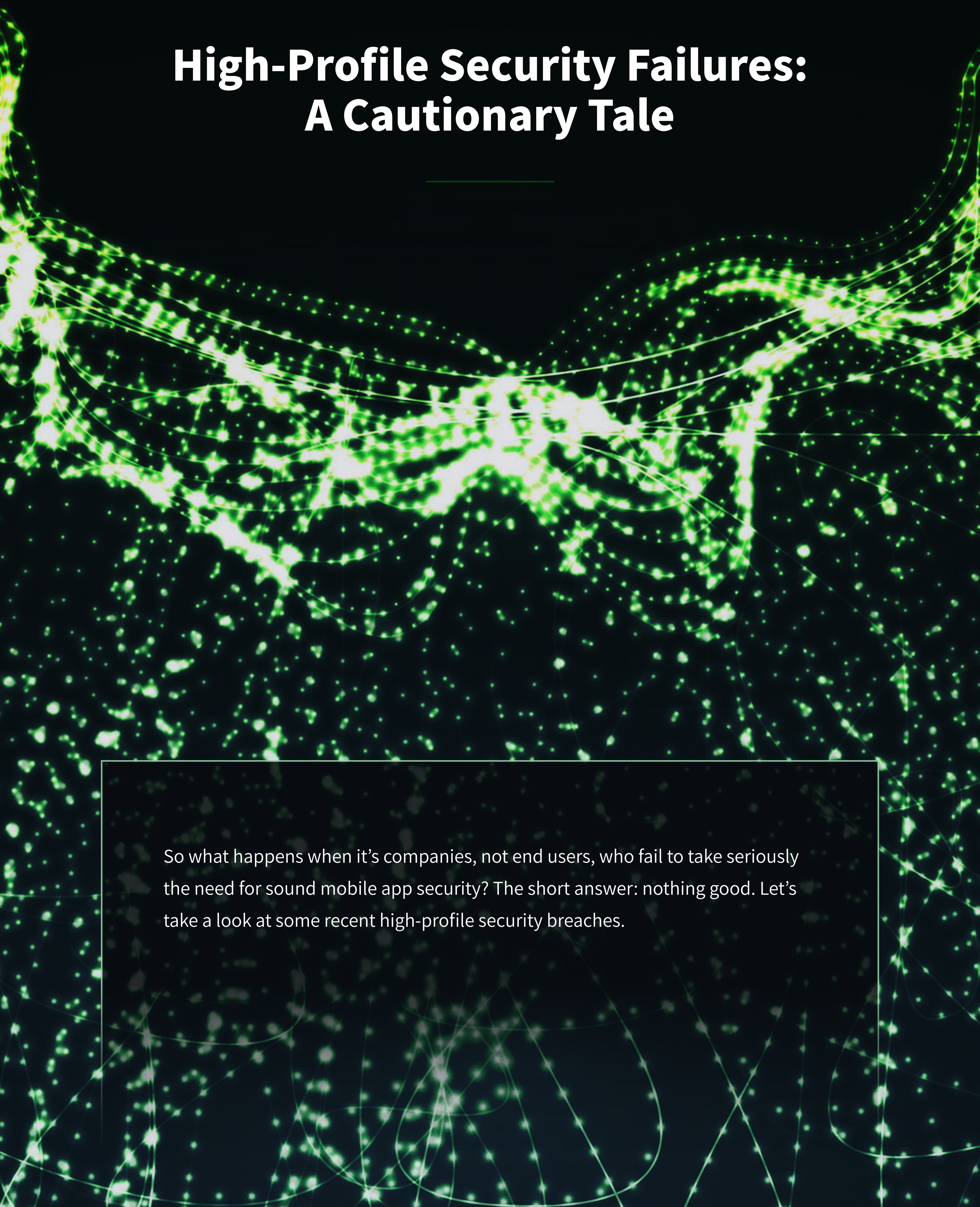
That’s where psychology plays a role. The beginning of the device security battle involves simply getting users to understand that security is important, then agree to adopt basic security measures, or to allow AppSolid to do it for them.

The right strategy varies from user to user and device to device. It can also change with the industry. Financial applications, for instance, demand much tighter security than a web-based game.

Some general rules for effectively implementing security include:

- Security updates need to be easy to install, hard to miss, and to not affect device functionality -- or, if they must, affect it only minimally.
- The easier a security measure is to adopt, the more likely a user is to adopt it.
- Convincing a user of the value of their data can convince them to embrace better security.
- Many users prefer an affordable program that will take care of things for them.
- The more frequently a user must deal with security issues, the less likely they are to remain up to date.

High-Profile Security Failures: A Cautionary Tale



So what happens when it’s companies, not end users, who fail to take seriously the need for sound mobile app security? The short answer: nothing good. Let’s take a look at some recent high-profile security breaches.

Starbucks

The Starbucks mobile app allows caffeine junkies to pay for their daily fix on the go. It was one of the earliest retailers to buy into mobile payment systems, and **now 29%** of Starbucks purchases are made through the company's mobile app. This made Starbucks a prime target for hackers.

Isolated reports of hackers accessing user accounts have circulated since 2015. Poor password protection, compromised devices, and behavioral engineering appear to be prime culprits. There's been little evidence that Starbucks' servers have been compromised. There's a lesson here for retailers: criminals don't have to hack into your information to harm your customers.

In early 2017, **a Buzzfeed reporter** uncovered a widespread scam for hacking Starbucks accounts. She received an email confirming a number of purchases she made. Except she didn't make those purchases at all. Thieves had compromised her account, taken it over, and began making purchases using the saved credit card information. **The source of the stolen passwords** appeared to be a third party vendor selling stolen passwords and other information.

This points to the very real dangers of online payment systems--particularly when they save credit card information or allow users to adopt lax security in the form of weak passwords. Even more salient, it demonstrates how a hack on one site can affect another. Gain access to a user's password, and odds are good they have used that password elsewhere.

WhatsApp

A WhatsApp security breach in early 2017 **may have left hundreds of millions** of accounts vulnerable to thieves. The breach allowed hackers to view users' messages and other private data if users clicked on a malicious file in a message. The attack also had the potential to allow criminals to access users' friends' accounts, including taking over their photos and other personal data.

The problem originated in WhatsApp's end-to-end encryption. This demonstrates, yet again, that encryption alone isn't enough. Without promptly addressing potential issues with their encryption, developers and app owners leave users with a false sense of security that can be exploited by criminals.

WhatsApp promptly fixed the problem, but **some analysts have raised other security concerns**. Those include unencrypted backup files of WhatsApp conversations and the way WhatsApp shares data with Facebook. In an increasingly connected world, a secure app may not be enough. App purveyors must also consider how users may render themselves vulnerable, how simple behavioral engineering tactics can render an app less secure, and how partnerships with third parties can compromise otherwise airtight security.

Equifax

Equifax, one of the world’s three credit reporting giants, put the data of nearly 150 million consumers at risk. The twists and turns grow ever more complicated. For now, the problem appears to be a tool the credit reporting giant used to build mobile applications. In other words, the problem was baked into Equifax’s apps from the beginning. Lazy app management and poor testing made data breaches virtually inevitable.

But that’s just the tip of the iceberg. We now also know that “admin” was the security login and password for at least one of its databases. If hackers knew where to look, they had to expend almost no effort to steal consumer data. This means there’s virtually nothing consumers could have done to protect themselves -- a hard lesson in how consumers suffer when companies don’t take seriously the need for excellent security.

Now, reports of identity theft, stolen credit, and compromised financial data are beginning to trickle in. Fighting these sorts of breaches is notoriously difficult, and the trickle may soon become a flood. We don’t yet know what will happen to Equifax, but if previous breaches are any indication, fines and litigation are a virtual inevitability.

Target

In 2013, Target inadvertently exposed the credit and debit card numbers, as well as names and mailing addresses, of at least 70 million consumers. The attack traced to a third-party vendor who was compromised. Hackers needed only to survey Target’s network to uncover the security hole. From there, it was easy to gain access to consumer financial data. Hackers wormed their way into Target servers to directly attack the retail giant’s point-of-sale systems.

Target first discovered the breach in November 2015, but waited until mid-December to report it, earning the ire of many consumers. We now know that much of the breach could have been avoided with better security, earlier reporting, better firewall protocols, two-factor authentication, and other well-accepted security strategies.

Target has **so far accrued** at least $300 million in lawsuit settlements thanks to the hack. And that figure may only go up with time.

ASHLEY MADISON®.COM

Ashley Madison

The site that bills itself as the Internet's premier location to start an affair didn't garner a lot of sympathy when word came that it had been the target of a massive data breach. Eventually, anyone who wanted could search the name of purported Ashley Madison users -- though some claimed that profiles were created without their permission.

The hack began when a mysterious team gained access to information about Ashley Madison and its users. The team demanded that the site be shut down. When Ashley Madison didn't comply, it released all of the data. Speculation continues to abound about how exactly the hack happened. It might have been a disgruntled employee who had access to significant data, making it clear how important it is to control your staff.

In the end, losers lost not only privacy and dignity, but also financial data. The hack released enough information to steal users' identities and financial accounts. Because that information is readily available, criminals can continue to mine it for nefarious purposes. It may be years before we really understand the full scope of the hack.

YAHOO!

Yahoo!

The **Yahoo! breach**, which compromised over 500 million accounts, may be the largest in cybercrime history. The hack gained access to user accounts, which then enabled hackers to contact users at recovery email addresses. This, in turn, offered them even more information, as panicked user's input passwords and other personal information in an attempt to recover their accounts.

Yahoo! believes that the breach was a government-sponsored one, though we don't yet know why or how the hack happened. Some analysts have expressed skepticism about Yahoo's claim that the hack was state-sponsored, citing ongoing security and personnel issues at the web giant.

Thanks to the hack, a bevy of personal data is now available for sale on the dark web. Because Yahoo was one of the earliest Internet companies, much of the data dates back 10 or more years, providing criminals with rich ground for digging through a person's entire life history.

Litigation in the case is ongoing, though Yahoo has fought efforts to put the case in front of a judge or jury. Ultimately, most analysts believe the breach could cost the company millions -- and potentially even bankrupt it.

A New Threat Every Day: Which One Will Target You?

So what exactly happens when a company or developer fails to properly secure their apps -- or when they don't take appropriate measures to encourage good consumer practices among consumers?

Sooner or later, they become a target. There's a criminal somewhere interested in every type of business and every type of consumer. And when the data is financial in nature, or provides detailed health records, access to powerful people, or personal information that can be used to steal an identity, there are many, many people eager to gain access. Let's review some of the most common data breach options:

- **Password brute force attacks:** When users select common passwords such as "admin" or "password," it's easy to break in. A dedicated hacker can simply try several passwords -- or write a script to continually try passwords until one eventually succeeds.
- **Behavioral engineering:** This is a strategy whereby a hacker or other criminal gets a user to give their information using simple psychological tricks. They might pretend to be a customer service representative, a family member in need, or even a law enforcement officer.
- **Phishing:** This classic scheme involves requesting passwords or other user information by pretending to be an email or other legitimate form of communication from the company that owns and operates the app.

- **Physical attacks:** When users leave their devices somewhere or the device is stolen, any information stored on the device becomes fair game. And often this information can be used to access data stored in the cloud.

- **Unencrypted code:** Coders still use unencrypted code, even though they know it's dangerous. Just don't.

- **Malicious lines of code:** A few decades into this digital experiment, code is everywhere -- and often free for the taking on message boards and in user groups. Savvy criminals can insert malicious instructions in seemingly innocuous code, causing developers to literally code the breach into the program itself.

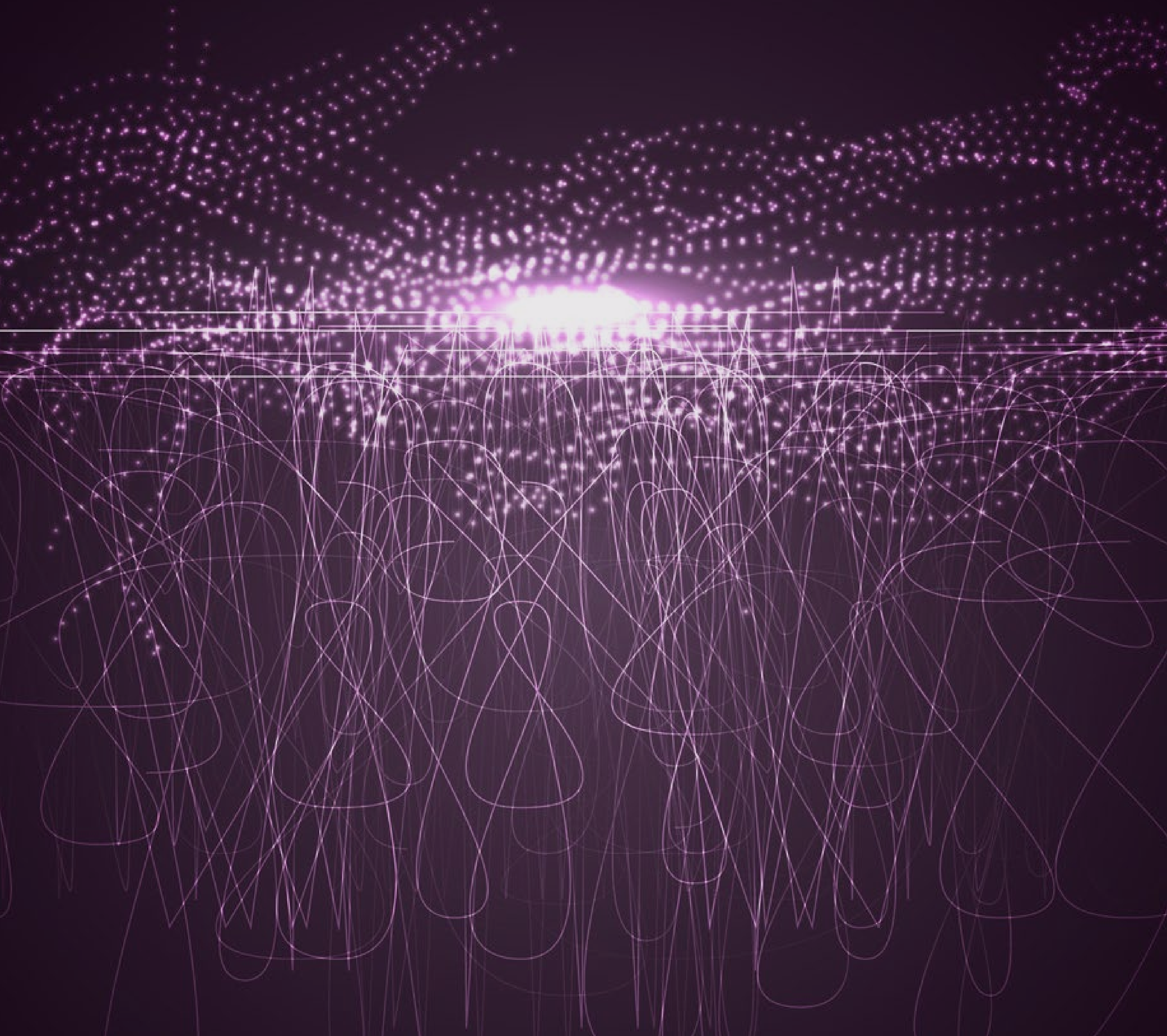
- **Device storage:** The more data stored on the device, the easier that device is to access. Simply physically taking the device may be all it takes. This is why programs that don't offer sufficient storage are asking for trouble.

- **Malware:** It's everywhere, and users may install it on their devices without even realizing it. The best malware operates in the background without disrupting the device, allowing criminals to steal information from the device for weeks, or even months.

- **Reverse engineering:** In this frustrating scenario, a hacker changes fundamental code or other information about your app, allowing them to control it -- and the users who rely on it.

This is just a broad overview; there are dozens of highly specialized techniques hackers can use to break into your app. If they're sufficiently motivated and your security is sufficiently lax, they're going to find a way in -- one way or another.

What Happens When Companies Don’t Implement Sound Security Practices?



So you understand that security is a concern. You know that consumers need better protections. But what does all this mean for you? Whether you're an independent developer, an app development company, a company offering its own internal apps, or a company that contracts with developers, you might feel like app security is ultimately a matter for consumers. Sure, you'll do the bare minimum. Anything beyond that is extra time and money that you just don't have.

Consider what happens to businesses that don't secure their apps:

- Their reputation gets dragged through the mud. Your good name is the most important thing you have. You spend money on advertising to cultivate it. Why would you throw it away? Think about how consumers viewed Target before and after the breach. Do you really want to be synonymous with bad security?
- They can face millions of dollars in lawsuits and legal settlements. They may pay millions more in attorney's fees and court costs.
- They can face government fines or regulatory actions.
- They may not have enough money to cover the financial costs they incur.
- They may have to spend millions to restore consumer data and fix the breach.
- They may lose money for their vendors, subjecting them to contract disputes and further lawsuits.

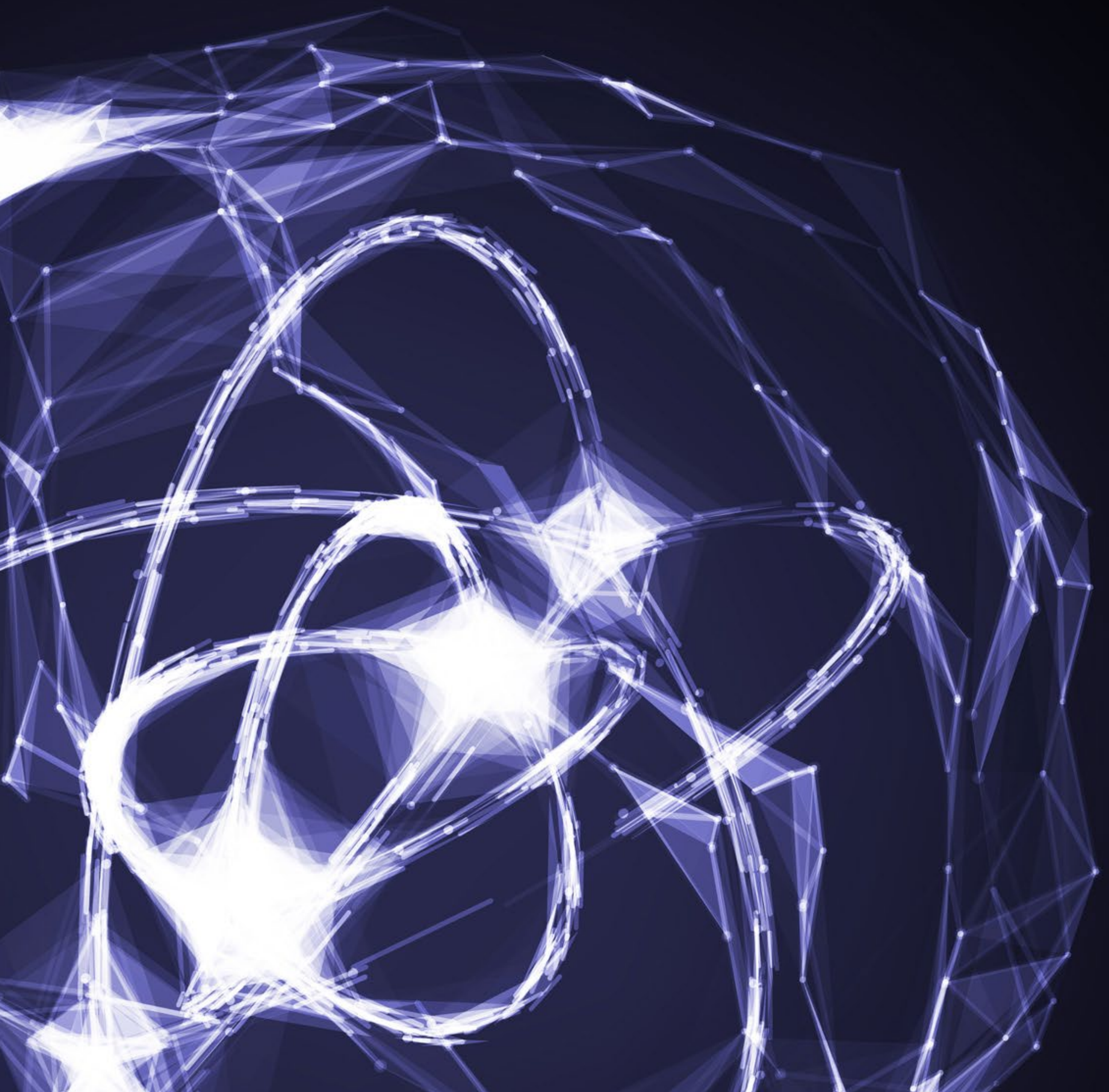
Your business can't afford this. Particularly when an affordable option like AppSolid is available. We offer industry leading binary protection that you and your customers don't have to think about. Gone are the days of challenging code writing to ensure security. We take care of it for you, so you can get back to running your business.

Mobile Security as a Competitive Edge

You know that not securing your apps can cost you money. But do you realize that sound security could also save you money? It might even help you edge out your competitors. Consumers are increasingly security conscious. But they don’t want to invest a ton of their own time and money. So if an app comes armed with excellent security they can trust, that’s going to immediately pique their interest. And if you can provide mobile security for a small price -- as you can if you use an affordable service like AppSolid -- that’s an offer an intelligent customer can’t refuse.

Don’t become one of the many companies falling on the trash heap of history thanks to poor security. Join the security revolution.

What You Must Do to Secure Your Apps



We already touched on the basics of mobile app security. You have to protect against threats internal to your company, against physical breaches, against behavioral engineering, and against every variety of virtual breach. Sound passwords and regular updates are a must. So too is an understanding of the specific threats your app is likely to face.

It's enough to make your head spin, but it doesn't have to be overwhelming. AppSolid's advanced protection offers cloud-based protection that you can trust. No more hiring a security guy you're unsure about. No more endless time spent writing code or updates. With AppSolid as your secret weapon, you can focus on what you do best: develop excellent apps. You deserve it, and so too do the consumers you serve.

Secure Your App
With AppSolid

Start Now

APP SOLID

help@appslid.co