# Credential Stuffing

Do you want to break a bad habit you might not recognize, even though it’s one of your worst? It’s not smoking cigarettes, eating junk food, procrastinating, or biting your nails — it’s reusing login credentials on websites. You didn’t see that coming, did you?

Using the same username and password over and over again is a bad habit most of us have. We just go with what we know — a nickname, the name of one of our children, a sailboat name, a sports franchise, something we can cue ourselves to remember — whatever, right? How harmful could it be? In the tens of billions of dollars is how harmful. This one bad habit is responsible for most of the security breaches on the internet.

## The Nature of this Habit

A lot of the internet is run on impulse, dopamine hits, and desire, whether it be consumer purchasing on Amazon or subscribing to a periodical that tickles your fancy. When we want something we’re in a state of high desire, and we’re far more likely to skip any action resulting from a thought process that takes us out of the impulse trance. The last thing on your mind when you’re signing up for an online subscription to *Sports Illustrated* and they’ve done a feature piece on your favorite quarterback is slowing the process down and being mindful of security, same thing when you're buying some new gear that's cutting edge for your gaming computer or a dinner set for your dining room table.

We’re creatures of impulse, slaves to the trance state induced by desire and the magic of advertising pioneered by Madison Avenue firms, and when we’re in this trance state we make mistakes. Remember the old Roman adage *caveat emptor*, which translates to buyer beware and means do your due diligence before purchasing something? In a digital age usage, it might also be applied to *secure* purchasing. Don’t rush the online purchase. Don't let the impulse guide you. Choose a secure username and unique password. Take your time, think, and breathe. The purchase opportunity isn’t going anywhere. It’s just the impulse talking, the desire.

## The New Caveat Emptor

People waiting to capitalize on impulse or addiction have been around since the human race started. It used to be just a two-party transaction, buyer and seller, the buyer looking for accurate information and the best price, and the seller wanting fair market value. The simple two-party intimacy of the consumer transaction is nostalgia on the internet. There are many parties now interested in your online purchase. They don’t have to be there at the time of the purchase. They can show up long after the transaction. The irrelevance of time is due to the particulars of online purchasing. The payment is digital. It goes from your bank account, credit card, Stripe, or PayPal account to the seller. You have to register on the seller’s website. You need a username and password to register. The username and password are stored on the seller’s website. That’s where the third party comes into play.

In the digital age, you don't see them. They’re not standing close to you. They don't engage you in conversation. They’re hidden in cyberspace, and they capitalize on your error at a future date when they’re plying their trade. The problem of reusing credentials is so endemic that a security industry term has evolved to describe an organized criminal enterprise, *credential stuffing*, or *credential stuffing attack*.

Caveat emptor no longer applies only to the buyer as a precaution against a duplicitous seller. It now allies the buyer and seller against third parties. Your bad habit is only part of the problem. The other part of the problem is not your fault. It’s the fault of the organization you trusted with your data. In their defense, the resources being applied towards their security are enormous, and they have to operate twenty-four hours a day, seven days a week from every corner of the planet. Digital space has no geography measured in kilometers. That should be self-evident to anyone who’s had a Skype call or a Zoom conference with people all over the world.

## The Breaches

There have been some enormous security breaches in the last decade. The most notable was Yahoo in 2013. But there have been some other big ones as well. Poor Yahoo gets kind of a bad reputation for being the first massive security breach. The Indian variant of Alibaba, called Aadhaar, had a data breach in January of 2018 that delivered hackers a treasure trove of information that included names, addresses, photos, phone numbers, emails, and most frightening of all, biometric data like fingerprints and iris scans. The breach affected over one billion people. Even more interesting is how the bad actors gained access. They went in sideways through an Indian public government database associated with a utility company.

. Alibaba itself got hit in November 2019. This one was an inside Job. A bad apple in the development department was working for a marketing company on the side and had been scraping customer data which included usernames and mobile numbers. He did this with crawler software he wrote himself. The developer and his employer were collecting the data for themselves. Nothing was sold on the black market. Both of them got three years in prison. In June of 2021, LinkedIn got hit. Data on seven-hundred million users was posted to a dark web forum in June of 2021. This impacted more than ninety percent of the user base for the LinkedIn application. It was hacked with data scraping techniques. LinkedIn played it down as a violation of its service contract but without any serious consequence to users. Their rationale was they *don’t collect sensitive data* on people. That may be true in the sense that there were no bank account numbers or no immediately profitable data that could be sold on the black market, but we’re talking about credential stuffing, and they got usernames and passwords. What LinkedIn is downplaying is that the login names and passwords of those seven-hundred million users probably allowed access to an exponentially larger number of websites that did have sensitive data. Think of it like a nuclear explosion. The actual mushroom cloud and the fireball are the nuclei of the explosion. We can compare this to the data breach at LinkedIn, but the electromagnetic wave that travels out for kilometers is the ancillary effect of the data hacked and all the other websites that are going to be hacked in the future as a result of credential stuffing. In April 2019 Facebook was hacked. It affected more than five-hundred and thirty million users. This breach included phone numbers, account names, and Facebook IDs. The data was posted online two years later. These are just a few of the massive data breaches that have taken place in the last decade. There’s nothing you can do to protect yourself from corporate breaches, but you can protect against attacks on other online profiles through good username and password habits.

## The Vulnerabilities

The attackers use automated tools like [Selenium](https://www.selenium.dev/), a browser automation development suite, [cURL](https://curl.se/), an open-source data transfer framework, or custom design tools if the sophistry is there. These tools go out and simultaneously automate the login attempt process on thousands of sites. If you’re in the habit of reusing usernames and passwords you increase the chance of a hit. It could be your bank account. It could be your Google account, which then gives them access to the Google stored passwords page on Google Chrome, then they have everything.

Credential stuffing attacks aren't the same thing as brute-force attacks. It’s all about checking the credentials they have against existing online services. Once they get your data they’re off to the bank. Then online purchasing begins. You wake up one day and your bank account is half gone. It’s a nightmare. Talk to anyone who has experienced it.

The five most vulnerable industries are online retail and e-commerce, video streaming services like Netflix, financial services and Banks, and higher education, and this one may seem out of place but it is, in fact, the richness of the data that makes this a high-value Target, and Healthcare organizations.

## The Solution

There are ways to protect yourself from credential-stuffing attacks. The most important defense is to break the habit of lazy usernames and passwords and repetition in usernames and passwords. But that only covers you. How safe can you be if the biggest online companies in the world can be breached? There is no defense against information theft if your information is in a big company that gets breached. All you can do is protect yourself from further damage resulting from credential stuffing attacks. Here is the common wisdom on how best to protect yourself.

Use multi-factor Authentication. Another way of looking at this is a two or three-step login process. For example, if the service provider offers a cell phone check-in with a pass code to augment your login, then use it. All you have to do is provide your cell phone number and every time you go to log in to the web service or site they're going to send a pass code to your cell phone as a text message. You simply apply the pass code to the appropriate field on the web page and gain access to the site. This will thwart any credential stuffing attack.

The rest of the defense unfortunately lies with the provider of the website or service. You can certainly write to their customer support department and demand that they provide security services, things like account lockouts and rate limiting, which set a limit on the number of times you can try to log in before the ability to log in is shut down. This is an excellent measure against credential stuffing attacks. Ask the service provider or website if they do credential monitoring. They can keep tabs on compromised credentials circulating on the dark web or being sold on black markets online. And ask the customer support department if they can use hCaptcha, a simple picture selection service that requires a conscious user and mitigates all credential stuffing attacks being done by an autonomous software system. Between the security of the website and the diligence you apply to unique usernames and passwords, you are about as safe as you can be.