# **The Online Gaming Platform Steam’s (by Valve) Data Breach Case**

At the very first weeks of November 2011, [Steam](https://store.steampowered.com/), an Internet gaming service, having popular games such as [Half-Life](https://en.wikipedia.org/wiki/Half-Life_(series)), [Counter-Strike](https://en.wikipedia.org/wiki/Counter-Strike), [Dota](https://en.wikipedia.org/wiki/Dota), was compromised by hackers in an illegal way which makes this a serious leak of data. The company [Valve announced](https://www.forbes.com/sites/danielnyegriffiths/2011/11/10/steam-hacked-newell-watch-your-credit-card/?sh=3ab8fe1532a0) that, roughly around 35 million users got affected by this breach. The leaked data was including usernames, hashed and salted passwords, game purchases, email addresses, billing addresses and encrypted credit card information.

Steam issued a statement saying that it saw no indications that the exposed credit cards were being used illegitimately but, it wasn’t enough for users to calm down and think in the same way at the time. Even from that, one of the users stated like, “My steam account is worth more than my bank account”.

The greatest danger was probably to those who had used the same password for their Steam and [Steam forums](https://steamcommunity.com/discussions/) accounts, or worse have been using the same password for multiple accounts, including their email. This is particularly dangerous as, along with probably providing a means to obtain passwords for every other online service connected to that address, it invalidates the [Steam Guard](https://help.steampowered.com/en/faqs/view/06B0-26E6-2CF8-254C#:~:text=Steam%20Guard%20is%20an%20additional,Steam%20account%20name%20and%20password.&text=When%20Steam%20Guard%20is%20enabled,login%20from%20an%20unrecognized%20device.) protection, introduced in March, which required verification by email whenever a user's Steam account is accessed from a new computer.

Valve's size and dominance in the [digital download market](https://colorlib.com/wp/platforms-for-selling-digital-products/), with over 30 million registered accounts, made this a source of concern. On the plus side, the evidence was at least that [Steam's identity protection](https://steamcommunity.com/app/238430/discussions/5/135511655650467945/) had been doing the right things in the event of a security failure. At some point, the way data is customer stored and associated was needed to be examined. But this was **not** the most crucial point.

## What Factors Lead Steam to the Data Leak?

* As a result of the security experts’ detailed research; found no evidence that the intruders took information from the database.
* The hack was not into directly to the main application, hackers got accessed to a **backup file** which washaving the four years long details between 2004 and 2008 of **all completed transactions**.
* Not having **a bridge financial online payment company** to have payments was also one of the important points to the harmfulness of the data leak.
* People who were not using [Steam Guard](https://help.steampowered.com/en/faqs/view/7EFD-3CAE-64D3-1C31) (which is one of another two factor authenticators) are the main victims in that case. Steam Guard was also notifying users if someone tries to log-in to their account from a foreign computer.
* The reason of not having as a requirement of using Steam Guard can also be accepted as another vulnerability.
* Valve’s use of forum software [vBulletin](https://www.vbulletin.com/) which had seen its share of security breaches in the past because of not having secure enough reach points.
* A message on the forums noted they were down for maintenance, but it turns they had received uninvited guests earlier after all.
* So, hackers got into the system/DB through ‘weak’ security of Steam’s forum which was built on vBulettin. And, people who were using the **same passwords** within the application and forum was in **more danger** than the ones using different passwords for both.

## **What Could Both Steam and Users do to Prevent the Leak?**

### **From the point of Steam**

* As being in the **first** rule of **OWASP Top 10 Privacy Risks**, **Web Application Vulnerabilities** impact one of the highest risks in cases like this. Steam’s forum page using vBulettin portal was the weakest point chose by hackers in this case. So, having end to end secure type of application could be the main precaution in this case.
* A self-hosted more secure and budgeted application would have a more secure way for Steam to go with.
* **Minimize Disclosure Point** -> The path hacker used through web application could be saved in a more hidden way.
* **Minimized Collection ->** As another point, credit card details also could be held by another secure financial company through the steps of payment.
* A password renewal rule within a specific time range could play a more private role to keep the user info in a safe place.

### **From the point of User**

* Most of the times, a password manager like [Bitwarden](https://bitwarden.com/) would use an essential role for the users to keep their passwords secure, and by being all different from each other.
* The users of Steam could use [Virtual Cards](https://blog.spendesk.com/en/virtual-credit-card) (a unique one or balance for each transaction) to do their payments, which would prevent this case from the beginning.
* Surely, as a **Minimized Retention** method, such as sharing not more than enough information with the site would put the user in a safer side, both on card information and personal information.

Refs:

1. [https://www.bbc.com/news/technology-15690187](1.%09https:/www.bbc.com/news/technology-15690187)
2. <https://venturebeat.com/2011/11/10/valve-steam-service-experiences-security-breach/>
3. <https://www.eurogamer.net/articles/2011-11-10-valve-confirms-steam-security-breach>
4. [https://www.businessinsider.com/steam-hacked-2011-11?IR=T](4.https:/www.businessinsider.com/steam-hacked-2011-11?IR=T)
5. <https://en.wikipedia.org/wiki/Valve_Corporation>
6. <https://steamcommunity.com/>
7. <https://colorlib.com/wp/platforms-for-selling-digital-products/>
8. <https://arstechnica.com/gaming/2011/11/valve-confirms-steam-hack-credit-cards-personal-info-may-be-stolen/>