SHIFT

# OUR PICKS FOR HATCHBACKS UNDER TK. 20 LAKH

ARFIN KAZI

Dhaka - the most popular city in the country, and also one of the most crammed cities in the world, leading to naturally heavy traffic at most times. Although sedans have always been the top choice in automotive commuting, hatchbacks have recently been hitting the limelight of Bangladeshis. Owing to their small stature, nimble shape and taking less space compared to sedans, they are steadily being a favourite among many fans. While there are plenty of good hatchbacks to choose from, here are our recommendations for hatchbacks under the Tk. 20 lakh price tag.

## Honda Fit (2017-2019)

**Price: Tk. 17 to 20 lakh** (reconditioned)

The Honda Fit is a great small car, 'fit' for Dhaka roads. Although it can be said that the Fit is not the most popular option in Bangladesh, it is one of the best cars to have due to its form factor and a healthy amount of torque to manoeuvre through thick traffic. The car also comes with a 1500cc engine and optional AWD, where FWD is the default. It is also quite fast in terms of speed compared to the other options in this list. Roughly priced around Tk. 17 to 20 lakh for the reconditioned ones, the Honda Fit is truly a bargain, offering good drivability and economy.


## Suzuki Swift (2017-2019)

**Price: Tk. 15 to 18 lakh**

The Suzuki Swift is a nice, small car with a great fuel economy of up to 20 kilometres per litre. It also has major safety features such as blind spot detection, lane assist and much more. There are plenty of models to choose from, namely the RS variant and the normal variant, both coming with a 1.2L 4-cylinder engine and an option for a gated manual transmission, which is rare in these times. Due to its affordable price range, it is the cheapest car on the list as well as one of the more practical options.

## Toyota Aqua (2017-2019)

**Price: Tk. 16 to 20 lakh**

This is a popular choice among most buyers, owing to Toyota building a stigma of trust among new car buyers. The Toyota Aqua is a small, peppy, hybrid car with a good amount of torque as well as fuel economy, being a hybrid. It averages around 25 kilometres per litre which is possible due to the clever aerodynamics to reduce the drag coefficient. The car comes with plenty of options and a 1NZ engine, which is known to be bulletproof and easy to work with. If you don't mind the car being just a little slower than the other options available, the Aqua is a great car to get for its price range.

## Toyota Vitz (2017-2019)

**Price: Tk. 18 to 20 lakh**

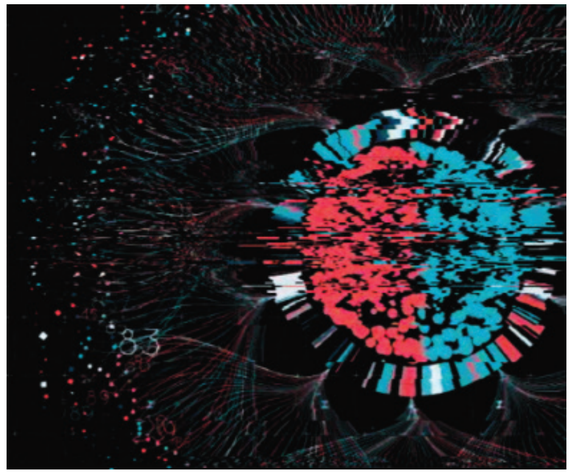
The Toyota Vitz is a very popular car among small hatchbacks which has options of a 1.0L version and a 1.5L version which is more widely available in the country. The car does not offer anything spectacular apart from the economy and reliability that Toyota is well known for. The Vitz sports no drama, except if you get the Jewela; which adds dark red trim pieces and a different fabric pattern on the seats. For the price range, it is a safe option to consider among the plethora of options out there.



# Key takeaways from the 2022 Data Breach Investigations Report

JINAT JAHAN KHAN

Every year, Verizon's 'Data Breach Investigations Report (DBIR)' covers an overview of global trends and patterns of data breaches, and cyberattacks across different industries. It is one of the most comprehensive reports that are publicly available online. For the last 15 years, these reports have been providing a place for security practitioners from where they can get real-world views on data breaches, cyber crimes, and data-driven analysis. The latest edition has examined 23,896 security incidents among which 5,212 cases were confirmed data breaches. The finding also highlights the common causes of such breaches and trendy attach vectors. Here are some key takeaways from the 2022 DBIR report.



**Common cyberattack vectors**

Regardless of which industry we are talking about, there are some common vectors for a breach of data. Broadly, these are the use of stolen credentials or weak credentials, human errors, ransomware attacks, and denial of service attacks. Credentials, phishing, botnets, and exploiting vulnerabilities are four main risks that can be found in all areas of the DBIR. No organisation is secured without strategies to handle each of these risks.

**Credential theft**

More than 80% of web application breaches were actually caused by the use of stolen credentials as per the 2022 DBIR report. Stealing credentials is the first stage of a credential-based attack. It allows cybercriminals to get access to someone else's accounts, passwords, and confidential data. These criminals then use such credentials to authenticate applications and steal the data of a concerned party. Credential theft has been behind some of the largest data breaches, such as the Equifax and Yahoo hacks.

**Human errors**

Humans are prone to make mistakes and errors, contributing to one of the biggest causes behind data breaches. According to the report, about 82% of data breaches happened due to human factors. It turns out that employees of large organisations play a significant role in such data breaches and cyberattacks by falling for phishing emails, misusing devices, and using weak or stolen credentials unconsciously.

Although the DBIR report has found that only 2.9% of employees clicked on phishing emails last year, the quantity is more than enough for cybercriminals to infiltrate the databases of large companies. Smart hackers know how to dump malware in the system as well as steal credentials with such underhanded phishing scams.

**Ransomware attacks**

Similar to previous years, ransomware attacks are still increasing in frequency by nearly 13% - for a total increase of 25% this year. The report notes that 14% of these ransomware incidents involve desktop sharing software. For instance, cybercriminals have used this strategy to exploit vulnerabilities in Microsoft RDP. On the contrary, 35% of them involved the use of emails.

**Denial of service attacks**

Denial of service attacks is one of the oldest attack patterns in the book. This is where an attack is meant to disable, shut down or disrupt a network, service or website so that intended users cannot use or access them. According to the DBIR report, there were 8,456 incidents involving denial of service attacks. But there were only four confirmed disruptions in business services that involved such an attack pattern. This may happen as this attack pattern does not aim to steal data. Rather, such attacks simply seek to disrupt or shut down business operations.

**Industry highlights**

Just like in previous years, the DBIR report has once again provided information on 11 specific industries. Apart from these, they have included a section regarding very small businesses (10 employees or fewer) for the first time. Some key observations are noted below.

In the accommodation and food services industry, threats from malware, and credential theft are still on the rise, but threats from system intrusions have been decreasing since 2016. On the other hand, the arts, entertainment, and recreation industry has faced most cyber attacks through system intrusion and basic web application attacks from financially motivated attackers.

Ransomware attacks are still on the rise in the education sector (more than 30% of breaches) along with the use of stolen credentials. Moreover, 40% of errors are caused due to sending wrong attachments or wrong emails to any wrong person or in this industry. With hope for financial gain, the financial sector is often attacked through phishing, using stolen credentials (hacking), and ransomware.

Internal actors in the healthcare sector and system intrusion in the information sector took the top spots in data breaches this year. Both the manufacturing industry and professional, scientific and technical services are subject to Denial of Service (DoS) attacks along with other common types of cyber attacks.

In the public administration vertical, the top spot in breaches is the system intrusion pattern where employees are seven times more likely to commit such breaches unconsciously than do them maliciously.

Lastly, both the retail sector and mining, quarrying, and oil and gas extraction companies are vulnerable to the same types of cyber attacks as last year, which includes credential theft, phishing, and ransomware attacks.

**Very small businesses are as appealing as large businesses to cyber criminals**

Whenever cyber crimes are reported in an organisation, it is common to assume that the target was a large organisation. However, even small businesses have become appealing to cyber criminals in recent years, and sometimes these businesses are more enticing than the large ones. Behind such acts, there simply is the "we'll take anything we can get" philosophy.

Another factor is that very small businesses with 10 employees or less are quite easy to target since they have very limited resources and generally cannot afford to have information security professionals or cutting-edge technology to protect themselves like large organisations.

**Best safety practices against data breaches**

Like previous years, the DBIR has also suggested some protective controls based on which types of breaches can mostly be seen across different industries. A protective control is a kind of broad theme or way to be safe against data breaches that again includes some security methods. These controls include security awareness and skill training for employees to be protected against cognitive hazards.

Another control 'data protection' aims to protect the organisation's data from accidental exposure through emails. Controls like account management and access control management help organisations manage access to accounts and the rights and privileges of users. Moreover, having a secure configuration of enterprise assets and software can reduce error-based breaches such as the loss of assets, misconfiguration, and so on.