Data Breaches – Is Your Privacy at Risk?

A data breach occurs when a hacker or a group of hackers accesses a merchant's network and steals their data. This data is either sold to the highest bidder or is leaked out into the internet.

Fraudsters and identity thieves are notorious for using data breaches to steal large amounts of money. They also implicate their victims with crimes they've committed, while they go scot-free.

Payment Gateway Breaches

Payment gateway breaches have been on the rise globally in recent years. Payment security protocols are unable to keep up with strategies which are employed by hackers and fail to prevent data breaches.

How Do They Work?

Payment gateways work by employing an SSL encryption. This transforms customer information into strings of code and sends it to the merchant's webserver.

Further, the customer's bank account receives an authorisation request and sends back a response code to its processor. The processor forwards its response to the payment gateway which is further sent to the website where it is interpreted.

This information is relayed back to the customer and the merchant. The entire process takes about 2-3 seconds.

How do Hackers Steal Your Data?

Mobile Banking Trojans

Trojans are piggybacked by viruses which are specifically designed to breach, steal and relay information back to a hacker.

How do these Trojans get into your PC/phone?

Fake Apps

A bank account usually supplies an official app for all your banking needs. Hackers create replicas of these apps and upload them to third party websites. Once you download the app and log in, your login credentials are sent back to the hacker.

App Hijacking

This is a sneakier version of the Trojan. They look like regular apps but have a Trojan installed within them. After it's installed, it scans your devices for banking apps. When it detects a banking app is opened, it puts up a window which looks identical to the bank app. If done smoothly enough, the user will not notice a difference. They enter their details into the fake login page, which are uploaded to the hacker.

Case Study – Credit Card Heist

On August 20, 2019, MasterCard Priceless Specials was breached. The hackers took sensitive information like credit card data, names, phone numbers, emails and IP addresses. This data was leaked on the data breach site; Have I Been Pwned.

According to its database, hackers have stolen the details of 89,338 German Mastercard customers with "Priceless Specials" accounts, with 46% of addresses part of this breach already having been added to the platform as part of previous data leaks.

The Hack of the U.S. Federal Reserve Bank, Cleveland, Ohio

One of the most noted hacks of this decade; Lin Mun Poo hacked into the Federal Reserve Bank’s computers in Cleveland and stole more than 4, 00,000 credit card numbers.

He was later arrested at the John F. Kennedy Airport almost a month later in a joint operation of the secret service and the NYPD. NYPD investigators issued a statement which states that suspect had travelled to New York to meet with other hackers to allegedly exploit some of the stolen information he had obtained.