**Why are hackers targeting food delivery companies?**

DoorDash, a food delivery company operating in the US and Canadian markets, announced in May 2019 that the company had been hacked and that the data of about 5 million users had been stolen. In March 2020, the German delivery service Takeaway.com, which operates with more than 15,000 restaurants, was hit by a DDoS attack. Using this tool, the attackers temporarily blocked the company's Internet connection and made the online service unavailable to users. In return, they demanded two bitcoins worth $11,000. In October of the same year, Chowbus, serving hundreds of thousands of customers in Australia, Canada, and the United States, was attacked by hackers. Another example: in May of this year, a group of hackers gained access to the data of 6 million Glove customers, including the data of couriers and other employees. The leaked information included the names, phone numbers, passwords, and payment systems of the victims.

As we can see from these examples, the development of this sector not only provides consumers with comfortable food but also becomes a convenient source of income for cybercriminals. The fact that customers for credit and debit card information are easily available to hackers through food delivery companies or restaurant chains is the main reason this area is attractive to hackers. Consumers can customize this with multi-factor authentication, encryption of sensitive data, and regular website and mobile app vulnerability checks.

So, Food delivery methods have increased in popularity in recent years. They've made it easier than ever to order food from your favorite restaurants, with just a few taps on your phone. This convenience, however, comes with the possibility of data privacy problems. When buyers provide private details such as their names, addresses, and credit card numbers, it is critical that their data is protected from misuse. In the following paragraphs, I'll examine the potential data privacy issues raised by meal delivery applications and provide examples of breaches of data that have happened.

**Examples of Data Breaches in Food Delivery Apps**

**1. DoorDash:** In 2019, DoorDash, a popular food delivery app, suffered a data breach that affected 4.9 million users. The breach occurred due to a vulnerability in the app’s third-party payment processor, which allowed unauthorized access to user data, including names, email addresses, delivery addresses, phone numbers, and hashed passwords.

**2. Uber Eats:** In 2020, Uber eats, a popular food delivery app, suffered a data breach that affected 100,000 users. The breach occurred due to unauthorized access to user data through a third-party service. The data that was exposed included names, email addresses, phone numbers, and order history.

**3. Deliveroo:** In 2021, Deliveroo, a popular food delivery app in Europe, suffered a data breach that affected 100,000 users. The breach occurred due to unauthorized access to user data through a third-party service. The data that was exposed included names, addresses, email addresses, and encrypted passwords.

**What kind of cyberattacks can the companies that provide this type of service face?**

Malware is one of the first ways used by hackers to target meal delivery services. They use a network flaw to install malware on the company's POS system. The programme then records every operation performed on the machine and sends it over the Internet to the attacker's site. In this case, the company should think about the security of its POS system as well as the protection of user data available on the website, including mobile applications. Users' confidence in the company may suffer as a result. This might result in a loss of customer confidence and, as a result, the company's reputation in local and global marketplaces.

The next cyber risk that companies in this service industry may face is phishing attacks. Such attacks are used by cybercriminals to induce employees to exchange network login information or other sensitive information. In this scenario, attackers send phishing emails with links that direct employees to malicious websites.

**Measures that can prevent cyberattacks.**

Cybersecurity experts advise on many measures to decrease the danger of data leakage in this service industry, including personal data.

The first step is to establish safe zones. Another strategy to avoid potential threats is to protect crucial control points. Monitoring system adoption to detect events at an early stage, improve management, and protect personal data in compliance with international standards such as GDPR and PCI-DSS can often restrict attackers' opportunities.

Also, regularly check and test mobile food delivery applications, using a properly configured firewall to protect devices from malware. Regulating peripheral compatibility (PCI) can be challenging, so food delivery companies can collaborate with IT professionals or utilize services from other services. These services can prevent material damage from cyberattacks and reduce reputational damage.

**Data Privacy Concerns with Food Delivery Apps**

1.**Gathering Data and Storage**: The amount of data that meal delivery apps gain from their customers is one of the key issues. While this data may be required to help the delivery process, it is critical that it is collected and stored securely. This includes ensuring that the data is encrypted and that only authorized people get access to it.

2. **Third-Party Access**: To facilitate the delivery process, multiple meal apps for delivery rely on third-party services. This means that data about users may be shared with these third-party services, which may have different data privacy policies and practices. Users should carefully read the terms and conditions to understand what their data will be used as well as who will have access to it.

3. **Illegal Access**: Another issue to be concerned about with meal delivery apps is the possibility of unauthorized access to user data. This might happen as a result of bad security behaviors such as weak passwords, insecure networks, and outdated software. App developers must employ strong security measures to prevent unauthorized access to user data.

**Protecting Your Information**

While data breaches are inevitable, there are steps you can take to protect your information when using food delivery apps. These include:

**1. Use Strong Passwords:** Ensure that one should use strong and unique passwords for each app you use. This will help to prevent unauthorized access to your account.

**2. Check Privacy Policies:** Always have to read the privacy policies of the apps you use to understand how your data will be collected, stored, and used.

**3. Enable Two-Factor Authentication:** Enable two-factor authentication wherever possible. This will add an extra layer of security to your account, making it more difficult for unauthorized users to access your data.

**4. Keep one Software Up-to-Date:** Ensure that your device’s software is up-to-date to prevent vulnerabilities that may be exploited by hackers.

Finally, food delivery apps make it easy to get food from your favorite eateries. They do, however, raise data privacy problems that consumers should be aware of. Users can safeguard the security of their data and prevent unauthorized exploitation by taking measures to protect their information.

**Prospective Customers:** Everyone who loves to eat and wants to get within some moments is our potential customers. All the customers will have their benefits once they just download our apps and create an account.

**Prospective Partners**: Those who will sell their food, we consider as our partners because they are the ones who are going to serve the customers, even have a plan that once we stand our company a bit then we will sell some shares to others so that even those organizations or people can contribute also with their expertise.