With cybersecurity landscape shifting all the time, threats are getting more sophisticated. For the financial and banking sector particularly, the stakes are quite high. This is because not only do they involve a large amount of money; they can also cause disruption to the entire economy in case of a cyber-crime.

According to a report by New York [Federal Reserve](https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf), financial institutions face 300 times more cyber attacks than other industries. This indicates how lucrative and attractive the financial sector is to the cyber criminals. Some of the reasons why it is important for banks to be vigilant about cybersecurity include:

* Weak cybersecurity practices can compromise the data and finances of customers
* An increase in cashless transactions means that more transactions now are digital than ever before.
* The costs incurred while recovering from a breach can be very huge and time consuming.

Banks need to inform regulators about any cyber incidents that can affect their ability to deliver products and services or come in the way of their operations. They also need to report anything that can affect the stability of the financial sector. These events could include ransomware attacks, hacking, Distributed Denial of Service (DDoS) attacks, or other similar threats.

**5 Biggest Cybersecurity Threats to Banks**

Let us have a look at 5 top threats that are faced by [banks](http://www.cardzgroup.com/BankCards.html) and other financial institutions.

1. **Ransomware and Malware**

Ransomware has affected many organizations around the world lately and it doesn’t look like the problem is going to stop anytime soon. It is a type of malware which encrypts important files and locks users out, making them inaccessible for everyone. The criminals then demand money or ransom to decrypt the data.

All end user devices like cell phones and computers can be a threat to your bank’s cybersecurity if they are infected with malware. When these devices connect to the bank’s network, it can attack the bank’s network and compromise customer data.

1. **Unencrypted Data**

Encryption is a very basic, yet very important part of cyber security. However, if the data stored on a bank’s devices is not encrypted, it can be a huge threat to the bank and an easy target for cyber criminals. Unencrypted data can be used by hackers right away. Therefore, it is important to encrypt all sensitive data of the bank so that even in case it is hacked, it cannot be misused by hackers.

1. **Cloud-based Cyber Attacks**

As more data and software systems are being stored in the cloud, cyber criminals are also seizing the opportunity to target them. Just like any other sector, banking and financial institutions are also a target of cloud-based attacks. They need to ensure that the cloud infrastructure they use is securely configured to be able to avoid potentially harmful data breach incidents.

1. **Social Engineering**

Social engineering is one of the biggest threats to a bank’s cyber security. It is a known fact that in most of the data breaches, people are the weakest link. They can be easily scammed into giving details of sensitive data, which can affect the bank’s employees or the customers.

Social engineering can take many forms. It can be done either through phishing attacks or by sending fake invoices that seemingly come from trusted sources. To avoid your employees from falling victim to social engineering attempts, it is very important to conduct regular security awareness training of employees and teach them about security best practices in daily work routine.

1. **Spoofing**

Spoofing is a relatively new type of cyber threat for banks. Cyber criminals impersonate the bank’s website URL with another website that looks and works exactly like the original website and redirect users to the fake website URL in different ways. When a user visits the fake website and enters their login information, hackers steal this information to use later. What is more alarming is that new spoofing techniques even allow hackers to use similar URL of the bank’s website and it is impossible for users to identify whether they are visiting the correct website or spoofed one.

**Conclusion**

As a bank, it is very important to be aware of threats to a bank’s cybersecurity and mitigate them while still providing the customers with uninterrupted and secure services.