In May 2014, eBay reported and released news about a loss of its database, which contains 145 million user information. They predicted lost data could be anything ranged from the user's basic personal details to critical information such as credit card. According to [1], the attackers had access to at least three corporate accounts and used the network to steal the data. By May 2014, eBay predicted that the attackers had had access for about 230 days, which means the attackers has planned the attack before October 2013. However, the real attack didn't occur until late February and early March. According to The Washington Post [2], once eBay acknowledged the vulnerabilities, they immediately send out the notices to all of its customers as they can't measure the scale of this attack. eBay only required customers to change their password. They might use the same password across other programs, software or platform and attackers could use that password and try break in [4].

Luckily, eBay later issues another statement claim that all of the user's payment information, including those who use Paypal as a payment method, is safe. eBay stored customer payment information in a different encrypted databased, which attackers didn't find out. eBay. As a well-known online marketplace, where it offers a variety of methods to the buyer and seller to sell and buy a product, eBay also suffers from controlling their customer. Quoted on Forbes [2], "eBay has long been saddled with a reputation for dodgy listings and phishing scams," As a platform for user interaction, it is very likely to experience some dodgy situation where it is out of control. Scams activity has occurred through the eBay platform .eBay has been striving to reduce the number of phishing scams from the user. .With this attack, it just makes eBay's reputation goes down even more. Customers who heard about the news began to lose interest and trust in eBay, where they will need to deal with some hassle such as credit card information change. eBay even lose more customers when they didn't offer any compensation to its customer about the attack, despite claimed responsible for the vulnerabilities. They didn't offer customers free credit monitoring, something that New York attorney court provided for eBay to provide to their customers [4]. A big company and corporation like eBay, a security attack, is a serious issue. They need to take it seriously. Things were quite lucky for eBay, with no security issue with all the payment information. Even more fortunate, after a few months after the breach, no fraud detected on any payment profile.

However, with this attack, it's also awake to all of the corporations and companies to treat their employee's accounts more secure to avoid such things like this happen. The employee account is very important. One account might not have full authorization to do a certain activity. The attacker can use that account to discover and explore the relationship and chain for other's accounts, and things could get complicated. Although it doesn't mean that company should only treat employee's accounts seriously, they also have to implement some security to avoid losing information as a chain like this. For example, doing 2-factor authorization would help reduce the number of unauthorized users accessing the account. Even if they have the information, it will report the owner right away if there is something suspicious.

[1]<https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>

[2]<https://www.reuters.com/article/us-ebay-password/ebay-asks-145-million-users-to-change-passwords-after-cyber-attack-idUSBREA4K0B420140521>

[3]<https://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/#52d74b9a7492>

[4]<https://www.businessinsider.com/cyber-thieves-took-data-on-145-million-ebay-customers-by-hacking-3-corporate-employees-2014-5>