Today, malware is the most dominant issue in the e-Business arena. It has affected many aspects of a business from the end user to online services. Malware has been so impactful that it has triggered responses to combat it. For the most part, these responses have been playing catch up. Some of these responses have not been sufficient enough to combat the malware. A lot needs to be done quick in order to stop the devastating destruction malware has on businesses.

E-Business has been very important in the 21st century because it has contributed greatly to the world economy. In order for an e-Business to thrive, it needs access to the internet and web for it to continue its growth. There are lots of positives that come from the web. Lately, e-business have been using Web 2.0 technologies to further grow their business. On the contrary however, this brings in negatives like malware. Malware has been so impactful on businesses that in 2007, it has done US$ 67.2 billion in damages directly and indirectly. In addition to this, businesses have invested US$ 7.8 billion to fix and repair all the damages that malware has cost them. Not only are businesses effected financially but the confidentiality of classified material can be stolen or the availability of data to be lost, could lead to theft of personal information about customers or staff of your organization. After all of those damages this could also lead to the brand being damaged as well.

Plenty of customers will now try to avoid a business if they have learned that their customers credit card information has been stolen. Some companies are risk of facing fines if they are unable to keep data from being breached. Adobe fell victim to this incident as they were fined US$ 1 million for a data breach back in 2013 for having more than 3 million encrypted customer credit card records were stolen. This will obviously result in a lost for business with the consumers. In 2009, Amazon and Walmart were both victims of a DDoS attack during the Christmas season. Both of their websites were taken down. Amazon and Walmart were eventually able to fix the problem but they already suffered from heavy losses from the attack. Amazon and Walmart are big enough to recover from these attacks. Small businesses however have a much harder time to recover and could potentially destroy the entire business. Most small business fall prey to ransomware. Experts in the information security field estimate that small businesses account for more than 60% of all malware attacks. On average small business lost over $100,000 dollars with in 25 hours of being infect of the ransomware. To prevent all of these attacks many businesses now invest in security to protect their business from further attacks.

Many of these attacks are carried out because of the end user. A Microsoft employee, Dandelion, said that weakness link to malware infection is human stupidity that lead to many successful social engineering attacks. Many business now take action to stress to their employees to practice good security habits through education and reminders to prevent further attacks. A lot of this includes reading emails carefully and report any suspicious email to the higher ups in your business. Small and large businesses install the latest versions of anti-malware software will help prevent any current mainstream malware attacks. With all that said, malware will always be ahead

in the game and business will always have to play catch up in order to protect their business and of their assets.