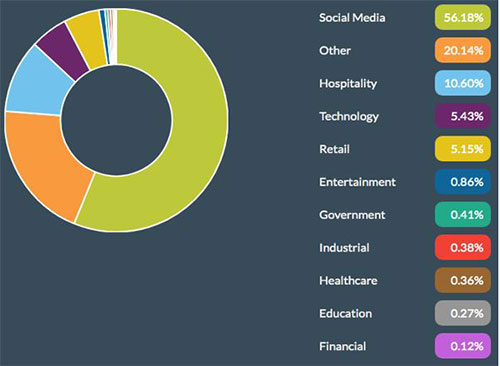
**Unit 2: Cyber Security Issues and Their Implications for Businesses**

Data breaching is when the safety of our information has been compromised and someone else has access to it. It allows unauthorized people from viewing secured data that we keep hidden. Reasons for this happening may include misconfigurations in the software, or losing hardware that may contain our personal data.

According to the Breach Live Index, 14,717,618,286 data records have been lost or stolen since 2013. Out of these, only 4% were those that had been encrypted and therefore the stolen data was useless. The pie chart below shows the percentages of data stolen from different industries.

Avoiding data breaches requires good cybersecurity practices. Some suggestions to avoid data breaches are:

* Only download registered software
* Update software when they biome old- newer versions tend to have more security upgrades
* Encrypt data — even if people manage to steal your data, they will not have access to it as it has been encrypted
* Use strong passwords and credentials for all of your accounts
* Change your passwords often and make sure they are strong and not easy to guess
* 

**Malware**

A Malware infection is a very common cybersecurity threat faced by thousands of internet users around the world. It may come from a multitude of sources. It works through different mediums such as pop-ups on web pages, spam emails, and downloads from unknown sources. According to the State of Cybersecurity, up to 36% of small to medium sized businesses suffer from malware infections.

How can Malware Infections be Avoided? There are many safety and security software available on the internet through verified sources that can be downloaded and used in all types of systems. Many email service providers incorporate virus scan and spam detection within their server — allows users to easily avoid malware infections. Do not open emails from unverified sources, especially if they are from people you do not know. Opening links that you get via email are usually a sure-fire way to get infected, so make sure you avoid doing so. Update and back up your computer regularly to make sure everything is up to date. If the computer is not updated, you might not be able to update your anti-virus software either, making you more prone to infections.

**Spyware**

Spyware or adware are types of software that track a user’s browsing history — they invade personal privacy. These show up as ads in sidebars on browsers or targeted ads. These can be avoided by not allowing permission to websites to track data. Firewalls should also be put in place to reduce data tracking. If adware is installed on your computer, not only could it be malicious, it can track data such as passwords, addresses, names, and other confidential information. Check your browser and computer settings to make sure your firewall is activated and you have a screening software activated that makes sure adware is blocked.

**Phishing**

Phishing is a form of social breach which come through in forms of instant messages and email. Usually, this makes you click on a link that tries to gain access to your personal information. The information is usually hacked into by redirecting the user to opening their bank account credentials on their bank site, or social media login details. This is extremely dangerous as it can leak information such as passwords, bank details, credit cards numbers, and house addresses. Many people have been victims to their information being used by others just because of clicking on unknown links. Phishing can be easily avoided by not opening links from people you do not know.

**Computer Viruses**

33% of all household computers are affected from viruses. A computer virus is perhaps the most common type of cybersecurity threat. It can start from altering a computer’s software to being a threat to its hardware. Computer viruses, like other cybersecurity threats, come from unknown links, adware, phishing, and clicking on unknown links. A computer virus can seep into your computer history and access saved usernames and passwords. This can be for anything from social networks to travel history details. It can also go into your bank account details, going as far as to using your bank account details to make purchases and transfers.While many of the cybersecurity threats come from the same places, they all affect computers and cybersecurity differently. The answer to protecting your system and security remain about the same throughout as well- keeping your devices up to date, ensuring the software come from authorized sources and are updated regularly, and installing a legitimate virus detector and anti-virus software for continuous online protection.