**Reasons why phishing attacks are successful**

Phishing is one of the most infamous cyber-attack vectors that is widely adopted by attackers for luring victims to reveal their sensitive and confidential information. This is generally carried out through emails. Attackers forge a fake email with a malicious link. Once that link is clicked and the victim submits his credential; game’s over. The person has been phished.

The history of phishing is quite old. It has been prevalent since the good old days of 90s. America Online (AOL) was one of the top internet service providers during the mid-90s with millions of visitors every single day. Attackers or ‘Phreaks’ (yes! That’s what attackers used to call themselves. Fancy, right?) started trading pirated software over AOL and formed a ‘warez’ community. This community stole AOL users’ passwords, created random credit card numbers and spammed users. This process was automated with the help of windows software AOHell. Once discovered, AOHell was shut down by America Online.

There are many cases that have been reported and even more that have not been reported. On an average, 1.2 million phishing attacks occur annually. According to the research done by Kaspersky Lab, phishing attacks almost doubled to 482.5 million from 246.2 million in the year 2017. Statistics show that phishing accounts to 91% of all the cyber-attacks. So, why do attackers use phishing attacks?

**Large User base:** One of the biggest reasons for the success of Phishing attacks is the widespread use of emails. At present, there are around 2.6 billion email users and this number is expected to cross 4.2 billion by the year 2022. Susceptibility rate of phishing attacks is quite high as attackers can easily find out email addresses, send phishing emails and there, it’s done.

**Humans are the weak link:** The other big contributor to the success of Phishing attacks is the victim itself. These days, social media has become a huge part of people’s lives. People are putting out their entire lives online. Attackers can easily access the personal information of the victim through social networking platform that helps in creating personalized phishing attacks (also known as Spear Phishing).

**Lack of awareness:** Lack of awareness amongst employees is also one of the major reasons for the success of phishing. In the recent years, attackers have shifted their focus from individuals to employees within organization. Statistically, 90% of the cyber-attacks are the result of employee negligence. During the year 2018, 76% increase in the number of phishing attacks was observed. 54% of the companies had experienced one or more attacks that compromised with their IT infrastructure and data. According to a survey by McAfee done on 19,000 people, approximately 97% of the people are unable to identify such attempts.

**Leniency in adaption of security measures:** The leniency in the adaptation of security measures is one of the biggest reasons for the success of phishing attacks. Studies have shown that organizations lag in spending money on the implementation of cyber security measures. During the year 2018, 51% of the organizations have made no change to the budget allocated to ensure cyber-security.

These reasons play a huge role in the success of phishing attacks. It is extremely important to ensure that cyber-security measures are adapted properly. Cyber security companies like [Kratikal](https://www.kratikal.com/network-penetration-testing.php), ensure that your network and infrastructure are secure from phishing attacks.