Phishing attacks have become very common in recent years. It all started 20 years ago, with AOL users being the first victims of it. In the early days of the internet, it was easy to detect fraud emails. With the passage of time, increase in email popularity led to an increase in phishing attacks as hackers were able to send automated emails with engaging subjects, hoping some people would click on the attached links. With the passage of time, hackers started to send emails from familiar companies or contact names. Then came the concept of spear phishing, where an attack is a targeted personalized email sent to specific targets.

**What is Phishing?**

It is a method to fool the target into providing their personal and confidential information or to infect files by inserting malware. Most of the times, Email phishing is used as a synonym for phishing but it’s not limited to that, neither is monetary gain always the desired outcome.

**History of Phishing - First Incident**

America Online (AOL) was amongst the biggest internet access provider in 1994-1995, with a consistent increase in users. At that time internet security was only considered important on government level and private businesses rarely invested in Cybersecurity. Due to this, AOL ended up being victim of phishing attack.

In 1994, a hacker named “Da Chronic” made an automated application called “AOHell”. One of its features was toolkit for phishing “CC/PW Fisher” that was used to exploit AOL’s messaging system. By sending a direct message to oblivious users, the hacker got access to personal credentials. The message was along the lines of being AOL representative, needing password and username for account verification. Users sent their personal information without becoming suspicious and became victim of the phishing attack.

Soon enough, the hackers targeted more valuable users, gave them threats to quickly verify their billing information otherwise their account would be deleted. Through this, the attackers were able to get victim’s bank account and [payment card](http://www.cardzgroup.com/ScratchCard.html) details along with their AOL credentials.

AOL then upgraded their Cybersecurity system. New measures were implemented to remove accounts associated with phishing.

**Data Leaks and Advancement in Phishing**

After AOHell’s success, phishing became a main hacking practice as it didn’t require any detailed knowledge of networking or programming. It took advantage of user’s insufficient knowledge about internet security and human error, and exploited human psychology alongside technology.

FACC an “Austrian aerospace parts manufacturer,” suffered a loss of over forty million Euros due to phishing. An employee received an email from the company’s CEO asking to send huge amount of cash to an undisclosed account as part of some “acquisition project”. Hackers spoofed CEO’s email and faked a new email. The employee fell prey to the attempt and disbursed the money. If Proper knowledge of Cybersecurity and phishing attacks was given to employee, it could have been avoided.

Both cases have a common thing between them. The hacker pretended to be another person to get whatever he wanted. Over the last two decades, only involved technologies got better. i.e. software for email spoofing that is used to send emails to a large number of users, and the quality of the content generated by the use of simple algorithms. On the flip side, training in cybersecurity domain has not improved and there’s a lack of in-depth knowledge in the subject, thus, lack of professionals in the field.

Social networks have made it easier for hackers to create an email that contains personal information of the receivers including their full name, home address and password of some accounts. Before this, forged emails used to begin with general greeting which was an indicator of fake email.

Lastly, data leaks are an important concept. Companies like Google and Facebook suffered from data breach over a year, even though they can afford to invest money into Cybersecurity. Previously, Myspace and Armor Games experienced data leaks and information was transferred to deep web. Currently, over two billion of the leaked credentials are being openly sold by hackers.

**Cloning Websites and Website Authenticity**

Increase in cloned websites was reported by the end of 2019 by APWG. In one of the attacks named Phish Phry, a fraud email (similar to that of the bank) was created and sent to users. The link redirected users to a cloned website of the bank. Any information that was input was collected and money was taken out of the accounts.

Cloned websites are taken down in a day, so they are hard to trace. In order to check the authenticity of the website, check if it starts with HTTPS or simple HTTP, the first one being legitimate. But some sites can gain SSL certificate due to weak rules.

**Phishing in Politics**

In 2016, John Podesta, candidate of presidential campaign of the USA, became a victim of Spear Phishing. In Spear Phishing, the hackers only target a specific person and not all the users. He received an email that was similar to the security alert of Google. The spoofed email contained multiple links that were shortened using Bitly service. A link took him to a website that was cloned, and he was prompted to enter his Gmail account credentials which resulted in several private emails being leaked.

In another instance, back in 2015, employees belonging to three companies distributing energy were targeted and became victim of Spear Phishing in Ukraine. They received and opened an email that had a BlackEnergy malware. This led to hacking of their information systems and the electricity supply to their customers was halted. The desired result in this attack was not to get hold of any personal data, instead it was to inject malware into the devices and serious damage.

Hackers can use Phishing both for stealing private information and infecting devices with virus which points towards poor security system. Companies of Cybersecurity are adding more and more websites that are cloned to their personal blacklists. In case of data leak, customers are informed. If people continue clicking on the infected URL and open attachments from suspicious addresses, phishing attacks will remain inevitable.

**New Phishing Techniques**

**Spoofing in Social Media**

In late 2016, Twitter accounts of customer service department workers of several banks in the UK were spoofed, as reported by Proofpoint. Cybercriminals copied the mannerism, naming conventions in use and visual assets of the employees of the banks.

Known as “Angler” Phishing, this type of attack is extremely efficient as customers are already anticipating a response from the respective brand. About 20 percent of all social media accounts of some global brands were reported to be fake by Proofpoint.

**Ransomware**

In Q1 of 2016, PhishMe malware review discovered that 92% of all emails recorded consisted of crypto ransomware strain which increased to 97% by Q3 of the year.

According to researchers, Locky is still the most flexible ransomware variant, where cyber criminals continuously refine the means of delivery.

**Tips to Prevent Phishing Attacks**

1. Do not reply to any suspicious emails and use spam filter for protection against spam emails.
2. Don’t click on links or attached media given in the suspicious emails
3. Use out-of-band communication to verify requests and information
4. Check browser settings to make sure Anti-Phishing services are turned on
5. Use different passwords for different sites by using password manager
6. Ignore any email requiring immediate action