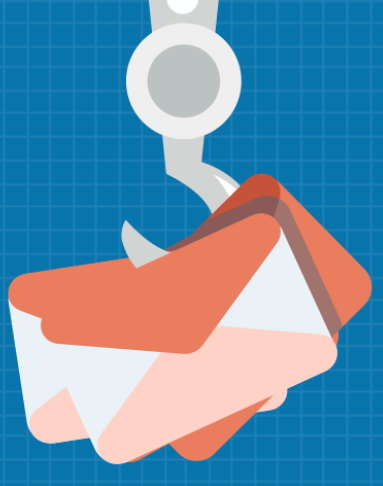
Phishing Attacks



What is Phishing?

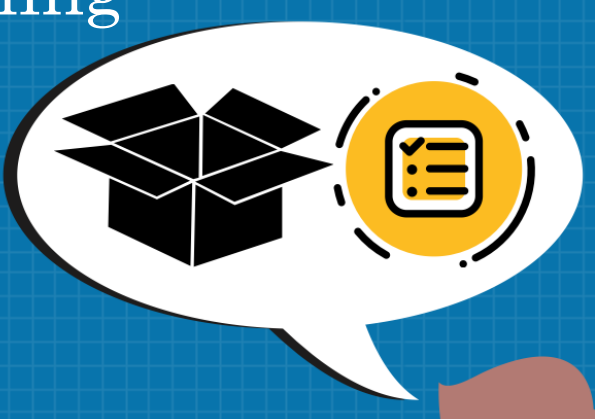
Phishing is a cyber crime in which the users are contacted by emails, phone calls or text messages to give their confidential information such as credit card details, passwords, bank details etc. This data is then used by the attackers to get access to target's personal accounts and may lead to financial loss.

85

Around 85% organizations suffered phishing attacks in 2016.

Common Phishing Attacks

1. Deceptive Phishing
2. Spear Phishing
3. CEO Fraud
4. Pharming
5. Dropbox Phishing
6. Google Docs Phishing



How To Avoid Getting Trapped?

Use spam filters to protect from spam emails.

Activate two step verification on your email accounts.

Do not enter login details on unsecured websites.

Set your browser's settings to avoid blocked websites.

Remember The Warning Signs

- Misspelled words or grammatical errors
- A URL that looks similar to original website's URL
- The email doesn't contain your name
- A mail or message that says you are involved in an illegal activity
- A website that claims to have found malware on your system

Phishing is the most common method to transfer malware through emails.

www.centextech.com

501 N. 4th Street,
Killeen, TX - 76541
Phone: (254) 213 - 4740

13355 Noel Road,
St # 1100, Dallas, TX 75240
Phone: (972) 375 - 9654

1201 Peachtree St NE400,
Atlanta, GA 30361
Phone: (404) 994 - 5074

Source: https://blog.barkly.com/phishing-statistics-2016