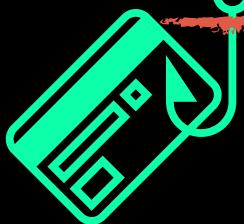


# PHISHING ATTACKS

---

# Explained

---



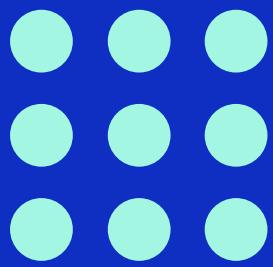


---

# Phishing Attack

---

Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels. The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims.



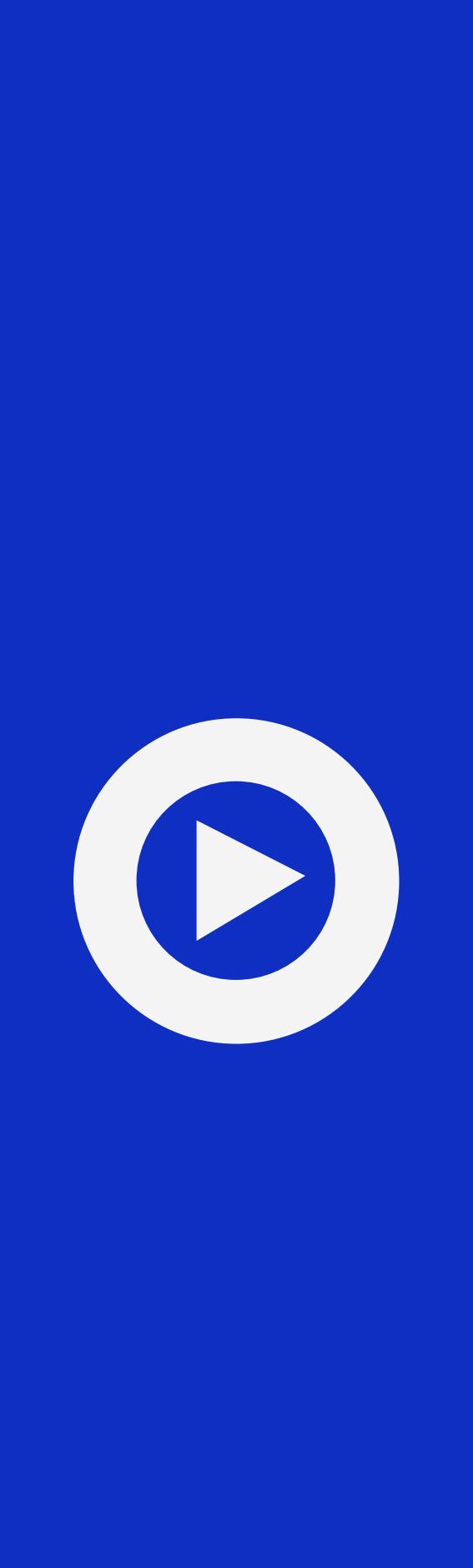
# 30%

of phishing messages get opened by targeted users

- **Verizon**

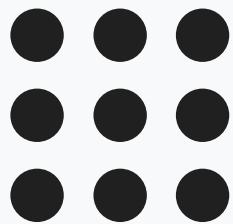
Did you know?





Around 1.5 Million new phishing sites are created each month.

- WEBROOT

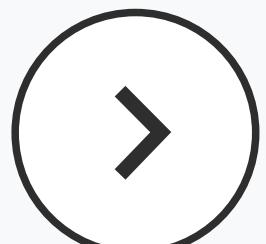


90%

Phishing accounts for  
90% of data breaches

# 6 TIPS TO PREVENT PHISHING ATTACKS

- 1** Be Skeptical
- 2** Be aware of your online presence
- 3** Inspect the links
- 4** Don't click the link
- 5** Be smart with your passwords
- 6** Keep your software updated



What is the single biggest mistake a company can do that makes them vulnerable to phishing attacks?





- When the company does not invest in the right tools and they do not provide proper training to their people about their role in information security.
- Browsing the internet carelessly.
- Not having proper policies that outline how to react to suspicious emails.
- When organizations are run in an authoritarian style where employees are trained to simply follow instructions, which leads them to easily giving up information.

- The same can be said for organizations that have a culture where asking for help is frowned upon.
- Not using a multi-layered approach to detect, analyze, and stop phishing attacks.
- Spear phishing is becoming more and more popular to target specific employees, so there is a bigger need to train employees about protecting their data.

**Follow us**



**Visit**

**Hackercombat.com**

# CONCLUSION

- The IT department can set up several layers of defense against such attacks, but each employee needs to participate in ensuring that all data is protected.
- Do not open suspicious emails, avoid browsing malicious websites, and never open an attachment from an email that you do not know the sender. These are just a few simple best practices that can be adopted by each employee in order to deter phishing attacks.

Follow us



Visit

[Hackercombat.com](http://Hackercombat.com)



# Hacker Combat Partnership

- Social Media Campaigns
- Sponsored Video
- Sponsored Article
- Sponsored Infographic
- Sponsored Multimedia Piece
- Banner Ads In Our Website
- Promotion Via Our Website



Increase brand awareness and drive  
revenue through **content sponsorship**

**Contact us at:**

**Partners@hackercombat.com**



**Follow us**