PHISHING ATTACKS :

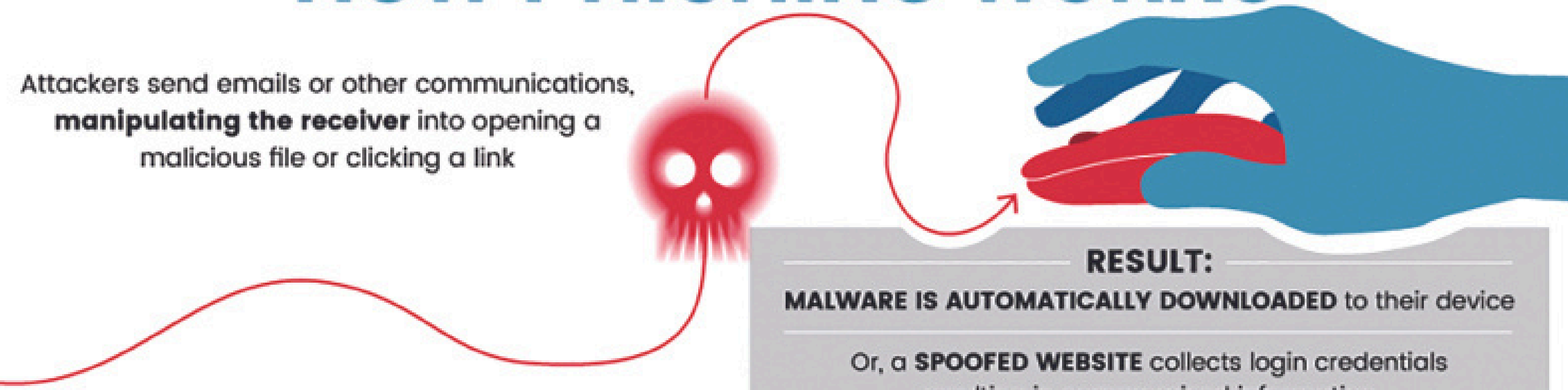
S T A Y S H A R P , S T A Y S A F E

WHAT IS PHISHING :

A cyber attack that uses disguised emails, websites or messages, to trick individuals into providing sensitive information, such as passwords, credit card numbers or personal details. The goal is to gain access to the system or to steal personal information for malicious purposes.

HOW PHISHING WORKS

Attackers send emails or other communications, **manipulating the receiver** into opening a malicious file or clicking a link



RESULT:

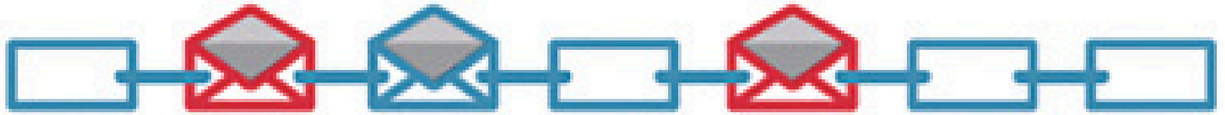
MALWARE IS AUTOMATICALLY DOWNLOADED to their device

Or, a **SPOOFED WEBSITE** collects login credentials resulting in compromised information

OVER HALF

of all phishing attacks contain malware

More than 2 in 3 phishing attempts used a malicious link



RESULT:

Fake Invoices paid, false bank transfers made

When someone clicks, the attacker gains prolonged access to the system —

On average less than 2 minutes after the email reaches the inbox

TYPES OF PHISHING

SOCAIL ENGINEERING

Manipulationg individuals to divulge confidential information

WEBSITE PHISHING

Fradulent websites imitating legitimate ones.

EMAIL PHISHING

Deceptive emails to extract information

PROTECTIONG PERSONAL INFORMATION

1. Never share passwords via Emails.
2. Use Two Factor Authentications.
3. Verify requests for sensitive information.
4. Be cautious with personal information sharing.

BEST PRACTICES FOR AVOIDING PHISHING

- Keep software updated and use security software.
- Educate and train employees.
- Regularly backup important data.

CASE STUDIES

Global enterprises fell victim to a phising attack as cybercriminals posed a trusted vendoor deceiving the finance department into urgently altering payment details for an invoice. The undetected fradulent payment led to financial loss and strained vendor relationships, only discovered when the legitimate vendor inquired about the overdue payment.

LESSONS LEARNED

Global enterprises strengthened vendor payment protocols with robust verifications and approvals. They introduced role-specific phishing training for the finance team, emphasizing red flag recogintion and trusted channels for payment verification.

FINAL WORDS

Phishing attacks will continue to happen in the future. It is upto the organizations and employees to learn from past mistakes and not repeat them. Employess can educate themselves on how to stop phishing emails. Organizations can deploy the best phishing protection solution to deal with such situation effectively. Furthermore organizations must include case studies related to past incidents in the employee education and training programs.

THANK YOU

ANGEL JOSEPH
ANGELJOSEPH114@GMAIL.COM

CODEALPHA REMOTE
INTERNSHIP