Are your employees the weakest link in your security strategy?

Do you need to know ?

What is Phishing ?

Nowadays environment, social engineering attacks are prevalent and increasing. The human element is often the weakest component in a company's security. Attacker know this and exploit it. 47% of cyber security attacks such as social engineering, spear phishing and ransomware attacks are that are financial motivated.

Phishing is a type of social engineering attack where cyber criminal send an email for attacking often used to steal user data, including login credentials, credit card number or other sensitive information. This is usually done by including a link that will appear to take you to the company's website to file in your information.

156 Million Phishing emails are sent by day

16 Million Phishing emails get through security filters and into inboxes

8 Million Phishing emails are opened

80K recipients Fall for a phishing scam

Phishing Simulation Service

Phishing simulation guards your business against social engineering threats by training your employees to identify and report them. Cybercriminals use phishing, the fraudulent attempt to obtain sensitive information, by disguising as trustworthy organization or reputable person in an email communication. Phishing emails are also used to distribute malware and spyware through links or attachments that can steal information .

Phishing Simulation Penetration testing comprises the techniques used by professional penetration testers to trick a customer's staff into revealing sensitive information or perform the action the create security holes for a hacker to slip through.

A penetration testers sends your employees email with link to files containing malware. For example, staff members may receive an email that informs them about their reward. The get the reward, staff members must click a link that gives the penetration tester access to the tar-

Phishing Simulation Benefits

Reduce the likelihood of attack via phishing

Tailored emails simulate 'real' attacks

Show improvements with granular reporting

Change user behavior with Awareness training

Save time and money

Real world and local scenarios

Find the vulnerabilities before Hacker can