

Outsmart Phishing: Stay Safe Online



What is Phishing?

Definition: Cybercrime where criminals trick people into sharing sensitive info. They pretend to be trustworthy sources, often through deceptive emails.

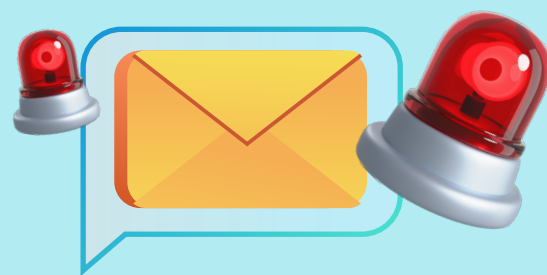


Understanding Phishing

- Evolution:** Phishing has evolved from simple, deceptive emails to more sophisticated scams.
- Phishing email anatomy:** Includes deceptive sender information, manipulative message content, and malicious links or attachments.
- Types of phishing:** Deceptive, Spear, Whaling, Cloning, and CEO Fraud, each with unique characteristics.

Recognizing Phishing Attempts

- Signs:** Common signs include urgent tone, misspellings, unrecognized senders, and suspicious links.
- Real-life example:** Snapshot of a phishing email, highlighting these common signs.



The Technology behind Phishing

- Forging emails:** Phishers manipulate email details to appear legitimate.
- Malware:** Malicious software that can infect devices, often hidden in phishing emails.
- Data capture:** Phishers profit from tracking and stealing personal or financial data.

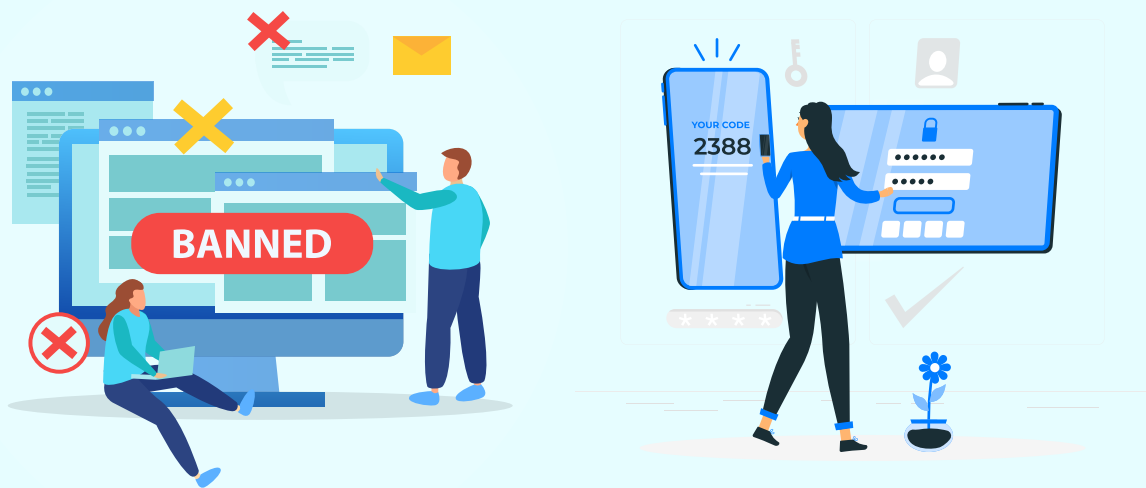


Protecting Yourself and Your Organization

- Steps for potential phishing:** Don't click on links, verify the sender, and report the email.
- Importance of security:** Regular updates, strong passwords, multi-factor authentication, and phishing awareness training.
- Role of filters and antivirus:** Can help detect and block phishing emails.
- Keepnet Labs' Phishing Simulator:** A tool for proactive cybersecurity training.

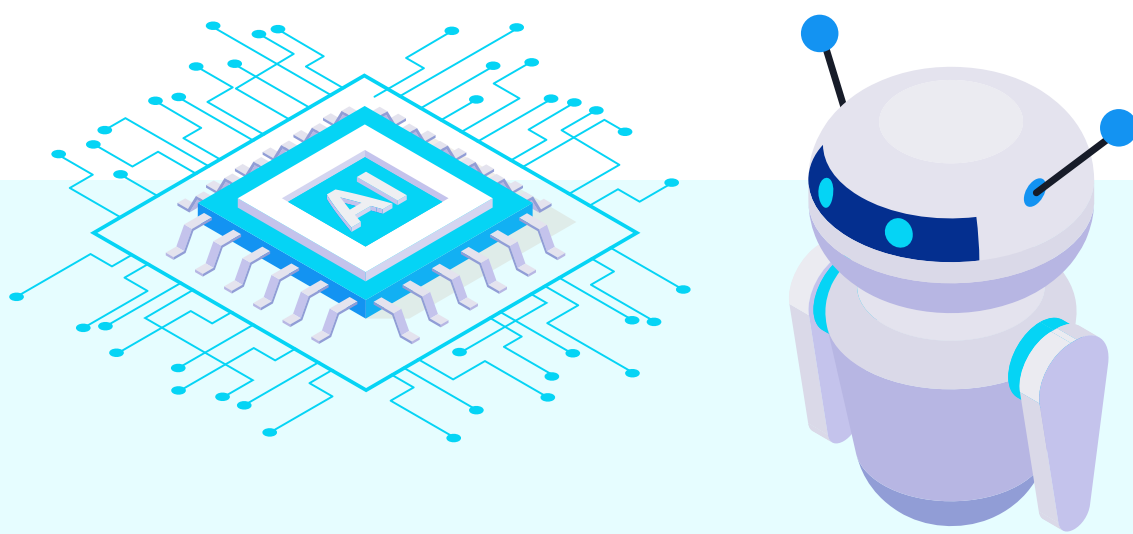
Reporting and Recovery from Phishing Attacks

- Report:** Phishing attempts can be reported to your IT department and organizations like the Anti-Phishing Working Group (APWG).
- Steps if victimized:** Disconnect from the internet, scan for malware, change passwords, and contact relevant parties (banks, credit bureaus).
- Recovery:** Damage control involves investigating the breach, restoring systems, and improving future defense.



The Future of Phishing

- Emerging trends:** Includes AI-powered phishing, mobile phishing, social media phishing, and Smishing.
- Future-proofing:** Stay informed, invest in employee education, upgrade security measures, and leverage AI technology.



Protect Your Business with Keepnet

- A comprehensive solution for phishing defense:** Keepnet Phishing Simulator is a tool that emulates phishing attacks, sending mock emails to employees to test their responses. Its purpose is to evaluate an organization's security efficacy, identify vulnerabilities, and educate staff. Start your **free trial** now.



Contact Keepnet Labs for more information!

     info@keepnetlabs.com