Anti-Phishing Scam Tools

Scott Reese
February 2025

This is a list of tools and techniques to detect, prevent, and mitigate phishing attempts.

1. Email Security & Phishing Detection Tools
These tools help filter and analyze emails for phishing indicators:
- Microsoft Defender for Office 365 (formerly ATP) – Protects against phishing, malware, and malicious links.
- Google Workspace Security – Includes advanced spam and phishing detection for Gmail users.
- Proofpoint Email Protection – Offers anti-phishing and threat intelligence solutions.
- Barracuda Email Security Gateway – Blocks phishing emails and provides anti-malware scanning.
- Mimecast Email Security – Uses AI and threat intelligence to detect and block phishing.

2. Anti-Phishing Browser Extensions
These help detect phishing attempts by warning users before they visit malicious sites:
- Netcraft Extension (Chrome, Firefox, Edge) – Alerts users of phishing websites.
- Avast Online Security – Blocks malicious sites and detects phishing attempts.
- Bitdefender TrafficLight – Provides real-time protection against phishing attacks.
- ESET Anti-Phishing – Prevents access to fraudulent websites.

3. Threat Intelligence & Monitoring Services
For advanced users, these tools help detect phishing domains, leaked credentials, and attack attempts:
- Have I Been Pwned? (https://haveibeenpwned.com) – Checks if your email/password has been exposed in a breach.
- PhishTank (https://www.phishtank.com) – A crowdsourced database of known phishing sites.
- IBM X-Force Exchange – A cyber threat intelligence platform.
- Cisco Umbrella – DNS-layer security to prevent phishing and malware attacks.

4. Network & Endpoint Security
These tools help prevent phishing payloads, malware, and unauthorized remote access:
- Cisco Secure Email & Web Security – Protects against phishing links and email threats.
- Palo Alto Networks Next-Gen Firewall – Detects and blocks phishing attempts.
- CrowdStrike Falcon – Endpoint detection and response (EDR) for phishing-based attacks.
- Microsoft Defender for Endpoint – Protects against phishing and malware on Windows machines.

5. Multi-Factor Authentication (MFA) & Identity Protection
To prevent credential theft in phishing attacks:
- Google Authenticator / Microsoft Authenticator – For securing logins.
- Duo Security – Provides MFA protection against phishing.
- Okta Adaptive MFA – Uses AI to detect suspicious login behavior.

6. Security Awareness & Training
Human error is a major factor in phishing attacks, so training is crucial:
- KnowBe4 – Phishing simulation and employee security awareness training.
- Cofense PhishMe – Helps organizations train users to spot phishing attempts.
- Proofpoint Security Awareness Training – Educates employees on recognizing threats.

7. Email Header Analysis Tools
To verify email authenticity:

- MxToolbox (https://mxtoolbox.com) – Checks email headers for spoofing.
- Google Admin Toolbox Messageheader – Decodes email headers to analyze origins.

Best Practices to Complement These Tools

- Enable SPF, DKIM, and DMARC for email authentication.
- Regularly update your software to patch security vulnerabilities.
- Use strong, unique passwords and a password manager (e.g., 1Password, Bitwarden).
- Stay educated on phishing tactics and share awareness within your friends and the membership.