HOW TO STAY SECURE
WHEN USING AI CHATBOTS

Artificial intelligence (AI) chatbots offer convenience, but they can also pose security risks. With the increasing use of AI chatbots such as ChatGPT, here's what you need to do to protect your data privacy and avoid a breach.

1. UNDERSTAND THE RISKS

- *Phishing Attacks:* Malicious bots impersonate legitimate services to steal your information.
- *Malware Distribution:* AI bots can be used to spread harmful software.
- *Data Privacy:* Sensitive information shared with bots can be intercepted or misused.

2. USE TRUSTED SERVICES

- *Verify Legitimacy:* Only use chatbots from reputable companies.
- *Look for Security Seals:* Ensure the service has appropriate security certifications.

3. SECURE YOUR PERSONAL INFORMATION

- *Avoid Sharing Sensitive Data:* Never disclose personal, financial, or login details to AI chatbots.
- *Use Strong Passwords:* Make sure your passwords are complex and unique.

4. UPDATE REGULARLY

- *Keep Software Updated:* Ensure your antivirus and other security software are up-to-date.
- *Check for Bot Updates:* Use chatbots that regularly update their security protocols.

5. MONITOR ACTIVITY

- *Regularly Check Statements:* Monitor bank and credit card statements for unauthorized transactions.
- *Stay Informed:* Keep up with the latest cybersecurity news to be aware of new threats.

6. REPORT SUSPICIOUS ACTIVITY

- *Contact Support:* If you suspect a bot is malicious, report it to the service provider immediately.
- *Alert Authorities:* Notify local or national cybersecurity authorities of any security breaches.

PHISHME COFENSE
EMAIL SECURITY