Phishing in Salesforce Email-to-Case

Status	In Progress
Priority	High
Target Audience	Enterprise/Corporate
Channel	Blog, Content Marketing, Email, Social Media

Challenges, Approaches, and Outcomes

The General Challenge

Salesforce Email-to-Case is designed to:

- Automatically convert incoming emails into cases
- Ensure fast response times
- Minimize manual handling

However, this creates a challenge when it comes to phishing.

The core problem:

> Phishing emails are treated like legitimate customer emails until someone manually intervenes.

This means that phishing emails can:

- Become cases automatically
- Appear in agent work queues
- Be opened under time pressure
- Be acted upon before being identified

The risk does not come from missing security tools, but from **where phishing detection happens in the process**.

Typical Enterprise Pain Points

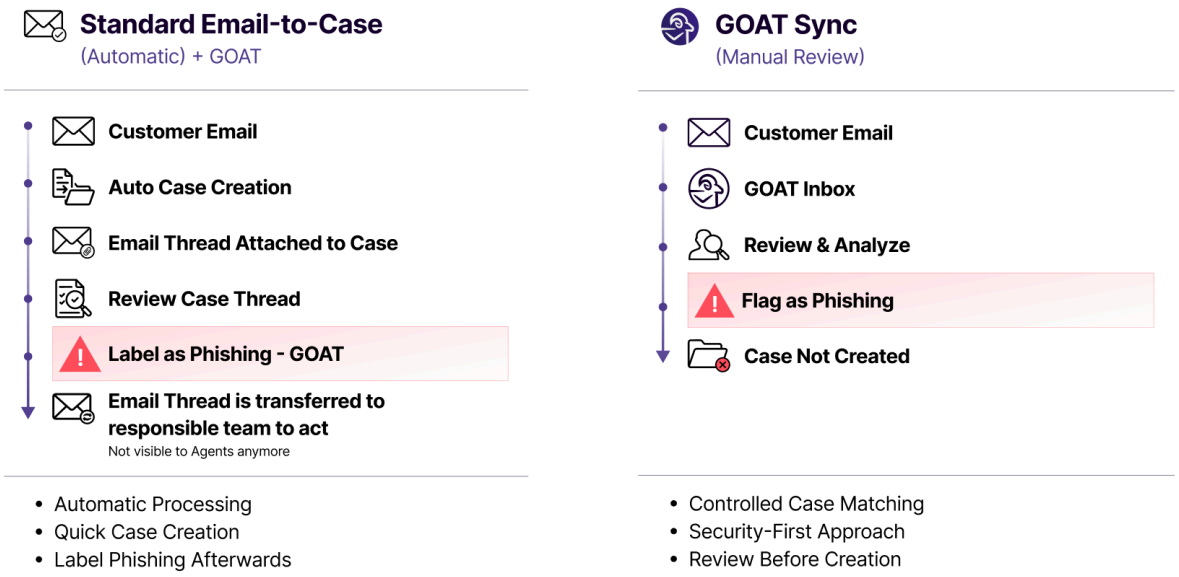
Across regulated and non-regulated industries, organizations face the same issues:

- Phishing emails enter Salesforce before being flagged
- Agents are expected to identify threats manually
- Reporting phishing is inconsistent or external
- Malicious emails become part of case history
- Security teams receive reports too late
- Audit trails are incomplete or fragmented

These issues exist regardless of industry or scale.

Two Approaches to Phishing in Email-to-Case

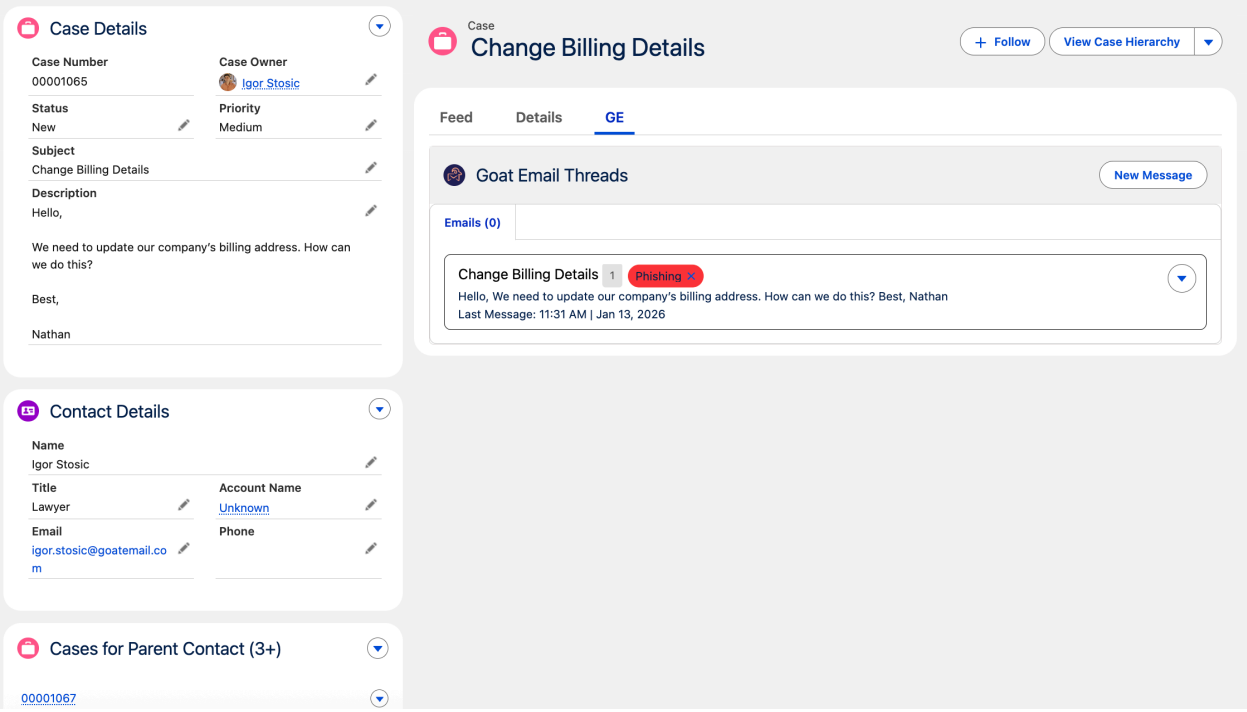
The visual above illustrates the **two standard approaches** organizations take when handling phishing inside Salesforce.



Approach 1: Automatic Email-to-Case + GOAT Email

How it works

1. Customer email arrives
2. Case is created automatically
3. Email Thread is attached to the case
4. Agent reviews the email
5. Email Thread is labeled as phishing and removed from Agent UI
6. Email Thread is transferred to responsible team to act (not visible to Agents anymore)



Benefits

- Fast case creation
- No delays in processing
- Minimal change to existing setup

Limitations

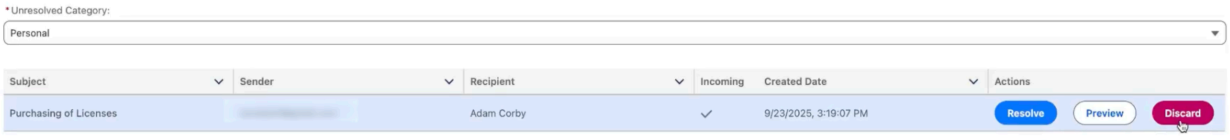
- Phishing emails already exist as cases
- Agents may interact with malicious content
- Attachments and links may be opened
- Cleanup happens after exposure
- Higher reliance on user judgment

This approach prioritizes **speed over prevention**.

Approach 2: Controlled Review Before Case Creation via GOAT

How it works

1. Customer email arrives
2. Email is received in a controlled inbox
3. Email is reviewed and analyzed
4. If phishing is suspected:
    - Email is flagged
    - Case is not created
5. Only safe emails become cases



Benefits

- Phishing stopped before entering case flow
- Reduced exposure for agents
- Cleaner case data

- Stronger security posture
- Clear audit trail

Trade-Off

- Slightly more controlled entry point
- Security-first design over pure automation

This approach prioritizes **prevention and control**.

What GOAT Email Enables

GOAT Email supports **both approaches**, allowing organizations to choose based on:

- Risk appetite
- Regulatory requirements
- Team maturity
- Use case criticality

Organizations can:

- Start with automatic processing
- Add phishing detection and reporting
- Gradually move toward controlled review where needed

This flexibility is critical in large enterprises.

The Outcome (What Changes in Practice)

Regardless of approach, organizations using GOAT Email achieve:

For Agents

- Clear visual guidance
- Less guesswork
- Safer interaction with emails

- Simpler reporting

For Security Teams

- Faster detection
- Better-quality incident data
- Consistent reporting
- Improved auditability

For the Business

- Reduced phishing risk
- Cleaner Salesforce data
- Better compliance posture
- Fewer security incidents

Key Takeaway

> Phishing protection in Salesforce is not about replacing Email-to-Case – it’s about deciding when and how emails are trusted.

GOAT Email makes this decision explicit, controllable, and auditable.
