InfoTank

PHISHING CASE STUDY

Phishing Attack Contained Before Internal Spread

February 2026

OVERVIEW

At one of our managed clients with nationwide locations, our advanced tools quickly identified a phishing campaign targeting their employees'. The messages originated from an external contact whose account had been compromised.

Our systems quickly identified that hundreds of emails were being sent within a short period of time, triggering a security alert.

Two employees opened the phishing email, which allowed the malicious file to begin spreading like a virus through trusted contacts. Our team responded immediately, contained the threat, and prevented further impact.

Because our monitoring identified the activity early, our team was able to stop the campaign before it could spread further inside the organization.

MALICIOUS ACTIVITY IDENTIFIED

Security monitoring identified indicators of a phishing campaign attempting to distribute a malicious file through trusted email relationships.

The following activity was detected:
- Large volume of emails sent in a short period of time
- Messages from a compromised external contact
- Malicious file attachment included in emails
- Messages targeting multiple employees

This type of activity is commonly used to spread malware by exploiting trusted communication relationships.

INCIDENT DETAILS

Location

Gilbert, AZ

Industry

B2C Service Industry

Potential Loss

Malware Infection
Credential Theft
Operational Disruption

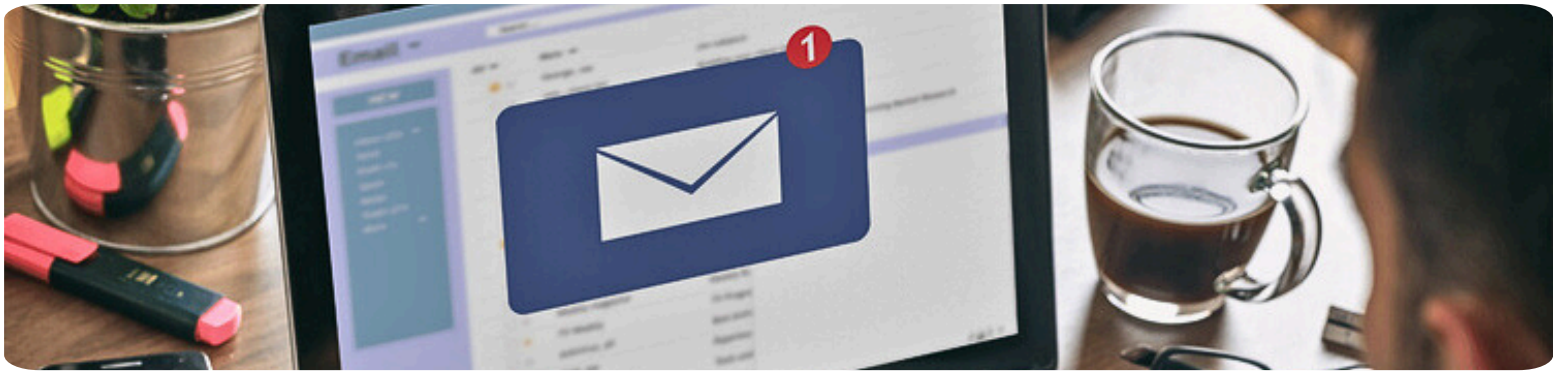
Status

Contained – No Client Impact



Phishing attacks often appear to come from trusted contacts. When an external account is compromised, attackers can send malicious emails that look legitimate.

When phishing attacks are successful, the hacker can usually gain complete control of admin accounts within minutes, giving them unlimited access to company emails and files.



Immediate Response & Business Impact Prevented

- ☑ No Malware Execution
- ☑ No Internal Spread
- ☑ No Data Loss
- ☑ No Business Disruption

- Malicious emails identified and analyzed
- Suspicious messages blocked
- Security alerts triggered by abnormal email volume
- Employees notified of phishing attempt
- Monitoring increased for additional activity

POTENTIAL IMPACT IF THE INTRUSION HAD GONE UNDETECTED

Malware Deployment	Credential Theft	Operational Shutdown
If the malicious file had been opened, malware could have executed on employee systems. This could have allowed attackers to gain access to internal systems and spread further throughout the organization.	Phishing campaigns often attempt to steal user credentials through malicious files or links. If successful, attackers could gain access to email accounts, internal systems, and sensitive company information.	Malware spreading through email systems can quickly disrupt normal business operations. Employees may lose access to critical systems, and recovery efforts can take significant time.
This could have resulted in significant financial loss for the business.	**Client and company data may have been exposed.**	**Entire business operations could have been halted.**

For more information, visit www.infotank.com or call: 770-450-8783, Email: ali@infotank.com

InfoTank