

# How to Secure Your Business Against Ransomware and Phishing



## What is Phishing?



Phishing is a social engineering technique used by cybercriminals to trick individuals into revealing sensitive information, such as login credentials, by using deceptive emails, text messages, etc.

## What is Ransomware?



Ransomware is a type of malicious software (malware) that encrypts a victim's files or locks them out of their own computer system. Once the files are encrypted, the attackers demand a ransom payment in exchange for providing the decryption key or restoring access to the system.

## Phishing vs. Ransomware

Phishing attacks often serve as the initial entry point for ransomware attacks. Cybercriminals commonly use phishing emails as a delivery method for ransomware. For instance, a phishing email might contain a malicious attachment or a link to a compromised website that hosts the ransomware payload. Once the recipient interacts with the phishing content, such as opening the attachment or clicking the link, the ransomware is downloaded and executed on the system. The interconnectedness between phishing and ransomware highlights the importance of comprehensive cybersecurity measures, including user awareness training, robust email filtering, regular backups, and strong network security, to mitigate the risks associated with both types of attacks.

## Why is it Important?



### Phishing

- Phishing and spoofing remain among the most frequently reported cybercrimes in the U.S. In 2025, the FBI received more than **180,000** phishing and spoofing complaints.
- Phishing and spoofing caused more than **\$215 million** in reported losses in 2025.
- Business email compromise caused more than **\$3 billion** in reported losses in 2025. These attacks often rely on spoofed or compromised email accounts to impersonate trusted contacts and trick employees into sending money or sensitive information.
- AI is making phishing easier to scale and personalize. In 2025, **84%** of phishing attacks analyzed by KnowBe4 used AI in some form, including AI generated content or automated personalization, up from 79.9% in 2024.
- AI is also making impersonation more convincing. The FBI received more than **22,000** AI related cybercrime complaints in 2025, representing more than **\$893 million** in reported losses.



### Ransomware

- Ransomware remains the leading threat to small and mid-sized businesses. It accounted for **70%** of Sophos incident response cases involving small businesses and more than **90%** involving mid-sized organizations.
- Ransomware continues to successfully encrypt business data. In 2026, **56%** of ransomware attacks resulted in data encryption, and only one in three smaller organizations stopped the attack before encryption.
- Recovery costs remain significant. The average cost to recover from a ransomware attack reached **\$1.7 million** in 2026, excluding the ransom payment itself.
- Ransomware can create costs far beyond the ransom itself, including business interruption, lost productivity, data recovery, incident response, reputational damage, and potential regulatory consequences.
- Paying a ransom does not eliminate the business impact or guarantee recovery. Organizations can still face **substantial recovery costs** even after a payment is made.
- Ransomware payments can also create legal and sanctions risks. Payments involving sanctioned individuals, organizations, or jurisdictions may violate U.S. sanctions regulations.

# Why Businesses Need Ransomware and Phishing Prevention



## Protection of Sensitive Data

Implementing robust prevention measures ensures the safety of your valuable data and protects your business from financial losses.



## Safeguarding Reputational Integrity

A successful ransomware attack or a high-profile phishing incident can severely damage your organization's reputation. By proactively preventing such incidents, you maintain the trust of your customers, partners, and stakeholders, safeguarding your brand's integrity.



## Regulatory Compliance

Many industries have specific data protection regulations and compliance requirements. Implementing comprehensive ransomware and phishing prevention measures helps you meet these regulatory obligations, avoiding potential fines and legal repercussions.



## Operational Continuity

A ransomware attack or a successful phishing attempt can disrupt your business operations, leading to downtime and productivity losses. By preventing such incidents, you ensure uninterrupted operations and minimize the impact on your bottom line.



## Cost Savings

The financial implications of a ransomware attack or a successful phishing campaign can be substantial. Investing in preventive measures is a proactive approach that saves your business from the significant costs associated with data recovery, incident response, legal actions, and potential ransom payments.



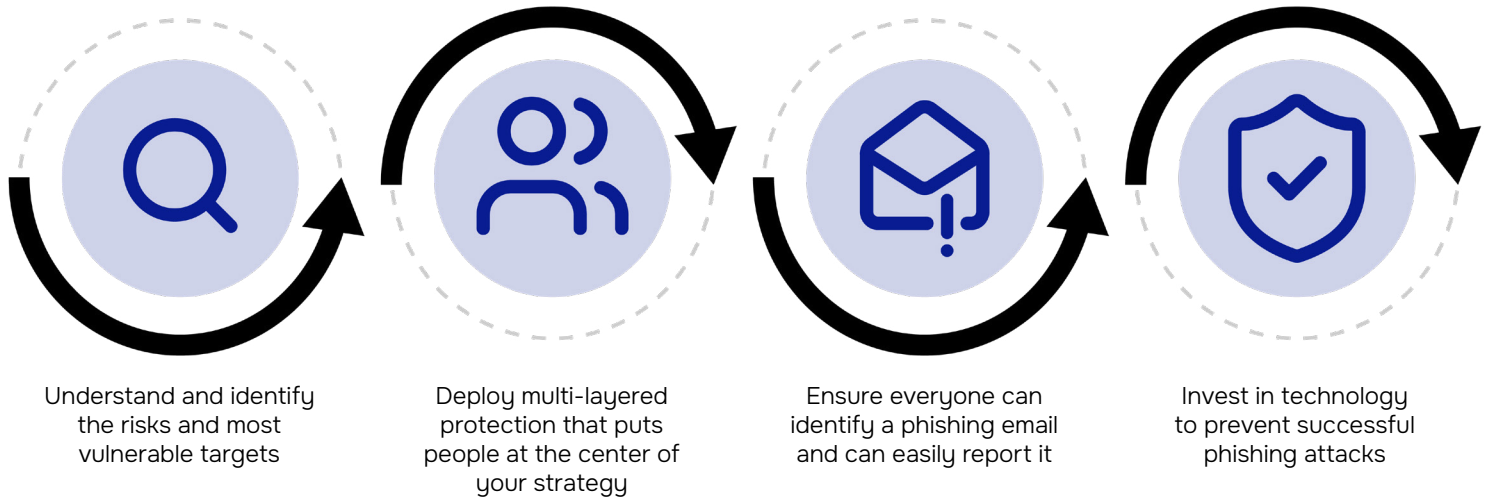
## Don't Wait Until It's Too Late!

Protect your business from the growing threats of ransomware and phishing attacks with our comprehensive cybersecurity solutions.



# How to Protect Your Organization

Phishing continues to be the number one cause of data breaches, and most phishing attacks start with an email. Strengthening your email security is thus one of the best investments you can make when it comes to your cybersecurity program.



1

## Strengthen Your Email Security With Inbox Detection and Response

**99% of malicious emails that bypassed existing security controls used social engineering or phishing links.<sup>6</sup>**

Deploy an intelligent system that empowers users to report suspicious emails directly from their inboxes. By leveraging advanced analysis and human expertise, potential phishing threats can be promptly identified, mitigated, and removed, preventing further damage. With one click, users can easily report potential phishing emails. Reported emails are quarantined and then scanned by software and SOC personnel to identify threats. Within just a few minutes, safe emails are returned to the users' inboxes, and all instances of malicious emails are automatically removed from all other users' mailboxes.

2

## Train Your Staff to Spot Phishing Emails With Cybersecurity Awareness Training

**After implementing Infosec training, Amway reported a 20% drop in its phishing rate and a 30% decrease in malware infected machines.<sup>7</sup>**

Educate your employees on recognizing and responding to phishing emails and social engineering tactics. By enhancing their security awareness, you create a vigilant workforce that acts as a crucial line of defense against cyber threats. We offer a fully-managed program that follows industry best practices and uses industry-leading training content. The program includes randomized phishing simulation emails sent to all enrolled users on a regular basis, as well as monthly training courses available in multiple languages. Weekly tracking reports are delivered to you via email to stay in the loop of your staff's progress.

3

## Regularly Back Up Your Data. And Don't Forget About Disaster Recovery.

**54% of organizations hit by ransomware used backups to recover encrypted data in 2025.<sup>8</sup>**

Regular data backup is one of the most effective ways to protect your business, since it allows you to restore your systems almost immediately without paying a dime. Even if your systems are compromised, you can restore important data and minimize potential damages. We offer a hybrid backup and a cloud-to-cloud backup for your Microsoft 365 environment.

With our Managed Backups & Disaster Recovery solution, your data is backed up both on-site and in a secure cloud location, providing extra security and redundancy. We offer flexible service packages with both standard and optional services to meet a variety of customer needs. Easily protect any physical, virtual and cloud infrastructure running on Windows, Mac or Linux, and spin up lost servers in seconds without the need for additional tools. Our team stands ready 24/7/365 to quickly respond to customer requests so that we can address potential issues to minimize the impact of a business-affecting event.

We also offer cloud-to-cloud backup to help protect data stored in Microsoft 365. Cloud data loss remains a significant risk, with organizations reporting incidents caused by accidental deletion, human error, external threats, and malicious insiders. Having data in the cloud does not eliminate the risk of loss or compromise. Microsoft 365's native capabilities are designed primarily around platform availability and retention, which can leave gaps in recovering customer data after deletion, corruption, or cyber incidents. With our Cloud to Cloud Backup, businesses gain an additional recovery layer for their Microsoft 365 environment. Our Cloud Backup and Disaster Recovery solution protects Outlook Email, OneDrive, SharePoint, Groups, and Teams data against loss.

## Other Measures We Offer to Strengthen Your Defenses



### Managed Endpoint Security

Protect endpoints with advanced threat prevention, detection, and response. Managed Endpoint Security helps identify suspicious activity, contain threats, and reduce the risk that ransomware or other malware spreads across your environment.



### Endpoint Management

Keep devices current with centralized patching and ongoing endpoint management. Regularly applying operating system and application updates helps reduce exposure to known vulnerabilities attackers may exploit.



### Managed Firewalls

Add protection at the network level by controlling inbound and outbound traffic, blocking malicious connections, and reducing unauthorized access to your network.



### Managed Security Service Edge (SSE)

Protect users as they access the internet, cloud applications, and private resources from anywhere. Managed SSE helps reduce exposure to malicious websites, risky applications, phishing attempts, and unauthorized access while applying consistent security policies across users and locations.



### Backup and Disaster Recovery

Maintain recoverable copies of critical business data so you can restore systems and reduce downtime following ransomware, accidental deletion, system failure, or other disruptions. A strong backup strategy can help reduce dependence on paying a ransom to regain access to data.



### Security Advisory Services

Strengthen the broader security practices that support ransomware and phishing resilience. TPx Security Advisory Services can help identify vulnerabilities, assess security posture, address compliance requirements, and develop plans and policies such as incident response and disaster recovery plans.

<sup>1</sup> FBI Internet Crime Complaint Center, 2025 Internet Crime Report, 2026.

<sup>2</sup> KnowBe4, Phishing Threat Trends Report, Vol. 6, 2025.

<sup>3</sup> Sophos Annual Threat Report: Cybercrime on Main Street 2025.

<sup>4</sup> Sophos, State of Ransomware 2026.

<sup>5</sup> U.S. Department of the Treasury, OFAC, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments.

<sup>6</sup> Fortra's 2025 Email Threat Intelligence Report

<sup>7</sup> Infosec

<sup>8</sup> Sophos, State of Ransomware 2025

