How to Secure Your Business Against Ransomware and Phishing

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.

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.

Ransomware vs. phishing

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 is the most prevalent cyber threat in the US [1]
- Phishing ranks as the second most expensive cause of data breaches—a breach caused by phishing costs businesses an average of $4.65 million [2]
- On average, data breaches caused by phishing took 213 days to be identified and 80 days to be contained. This means that the average time it takes to contain a phishing threat overall is 290 days. [2]
- At least one person clicked a phishing link in around 86% of organizations.[3]

Ransomware

- Ransomware remains the most common cyber threat to small and medium businesses (SMBs), with 60 percent of MSPs reporting that their SMB clients have been hit as of the third quarter of 2020 [4]
- Two out of three mid-size businesses have suffered a ransomware attack in the last 18 months [5]
- Ransomware attacks are becoming more frequent and sophisticated
- Ransomware can cost businesses in many ways aside from the ransom payment itself, including reputation damage and downtime costs
- Making a ransomware payment is actually illegal as of a 2020 ruling by OFAC and FinCEN
- Payment doesn't guarantee all your data will be restored. The 2021 State of Ransomware Report found that, even after paying, only around 8% of victims recover all of their data. The average ransomware victim loses around 35% of their data.

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.

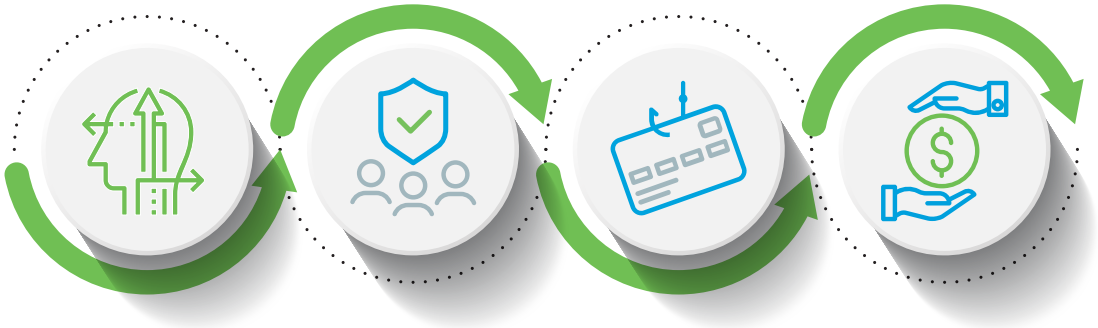
Operational Continuity A ransomware attack or a successful phishing attempt can disrupt your business operations, leading to downtime and productivity losses. By preventing such incidents, you ensure uninterrupted operations and minimize the impact on your bottom line.

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.



Understand and identify the risks and most vulnerable targets

Deploy multi-layered protection that puts people at the center of your strategy

Ensure everyone can identify a phishing email and can easily report it

Invest in technology to prevent successful phishing attacks

1 Strengthen your email security with Inbox Detection and Response

91% of all attacks begin with a phishing email.[6]

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

84% of U.S. organizations said security awareness training has reduced phishing failure rates, the highest of any country surveyed.[7]

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.

For a limited time, get TPx's Managed Inbox Detection & Response, Security Awareness Training, and Cloud-to-Cloud Backup for just $8/user/month

New customers only, or if an existing TPx customer, must be new to the services in the bundle (no renewals)

3 Regularly back up your data. And don't forget about disaster recovery

60% of SMBs that lose data will shut down within 6 months — yet 75% of small businesses don't have a written disaster recovery plan.[7]

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-effecting event.

We also offer cloud-to-cloud backup to secure the data in the cloud. Cloud data loss poses a significant risk, with more than 75% of such incidents attributed to human causes like mistakes and malicious attacks. Having data in the cloud doesn't necessarily protect you from these cyber threats. Microsoft 365's built-in disaster recovery measures primarily address infrastructure failures, leaving a critical gap in protecting customer data. With our Cloud-to-Cloud Backup, businesses can bridge this gap, safeguarding their Microsoft 365 environment against loss and ensuring ongoing productivity. Our Cloud Backup and Disaster Recovery is a comprehensive backup solution that protects Outlook Email, OneDrive, SharePoint, Groups, and Teams data against loss.

Other measures we offer to strengthen your defenses

Advanced Threat Detection Utilize cutting-edge technology and automated machine learning engines to detect and identify sophisticated ransomware and phishing attempts. Stay ahead of evolving threats and ensure timely response to potential attacks.

Endpoint Management & Security Regularly updating software and operating systems is essential for addressing vulnerabilities that attackers may exploit. With centralized patch management, it's easier to keep all endpoints up to date with the latest security patches and bug fixes. Patching helps to close security loopholes and minimize the chances of successful phishing and ransomware attacks.

Firewall and Network Security Implement a next-gen firewall solution that monitors and filters incoming and outgoing network traffic. This helps prevent unauthorized access, blocks malicious connections, and fortifies your network against ransomware attacks and phishing attempts.

Security Advisory Services We offer free ransomware evaluation — and a more comprehensive ransomware assessment (for a fee). This assessment focuses on the aspects of cybersecurity that have the highest value in defending your organization against ransomware attacks.

[1] FBI's IC3 2022 report [2] IBM 2021 Cost of a Data Breach
[3] CISCO's 2021 Cyber Security Threat Trends [4] Datto
[5] 2022 MSP Threat Report [6] Proofpoint's 2022 State of the Phish Report [6] PhishMe Report [7] Clutch & Nationwide Insurance