opentext™

Protect your organization from ransomware and phishing: A practical cyber-defense guide

Simple, layered protection for small and medium businesses to guard against email-borne threats, account takeover, and ransomware

Contents

Small and medium businesses face growing risks from ransomware and phishing attacks. Cybercriminals increasingly target SMBs because limited resources and smaller security teams make them vulnerable. A single phishing email or malicious link can lead to credential theft, account takeover, and ransomware infections that cause costly downtime, data loss, and reputational harm.

This guide explains how SMBs can build a layered cyber-defense strategy that is practical and effective. It covers prevention, detection, user education, and response steps tailored for organizations without large IT teams but still requiring enterprise-grade protection. By combining technologies such as endpoint security, DNS filtering, email threat prevention, encryption, and continuity, SMBs can achieve resilience without complexity.

Why email is your greatest risk

Email remains the most common entry point for phishing, business email compromise, and ransomware. A single click on a malicious link can compromise credentials or install malware. Solutions like OpenText™ Core Email Threat Protection apply multiple layers of defense, including URL rewriting, attachment sandboxing, and message retraction, to block threats before and after delivery. Internal emails are also safeguarded to prevent lateral phishing and impersonation attacks.

Protect sensitive data with email encryption

Email security is not only about blocking threats; it is also about protecting content. OpenText Core Email Encryption automatically scans outgoing messages and attachments, encrypting or quarantining them based on policy. Multiple delivery options ensure compatibility and dashboards provide visibility into encryption triggers and policy compliance.

Ensure email continuity during outages

Email downtime can disrupt operations. OpenText™ Email Continuity allows users to read, reply, and compose messages through a secure portal when mail servers fail. Once systems recover, all activity syncs seamlessly.

Maintain privacy and control over email content

For large or sensitive file transfers or legally binding e-signatures, OpenText™ Core Email Message Privacy enables secure delivery through a web portal. Businesses retain control over viewing, forwarding, and downloading, with the ability to revoke access and track activity for compliance.

Resources

Request a call or demo

Learn more ›

Layered defense for SMBs

A strong SMB cyber-defense strategy includes:

- ✓ Endpoint protection to block malware and ransomware before they execute and provide rapid detection and response.
- ✓ DNS protection to stop access to malicious domains before connections occur, reducing infection risk.
- ✓ Security awareness training to educate employees on phishing and social engineering tactics.
- ✓ Email security solutions to protect inbound and outbound communications.
- ✓ Managed detection and response (MDR) for 24/7 monitoring and expert threat hunting without the need for an in-house security team.

Cyberthreats are not limited to large enterprises. SMBs are prime targets, but with a layered approach, businesses can defend effectively without overwhelming resources. OpenText delivers a unified, cloud-native cybersecurity platform designed for SMB needs, combining advanced technology with expert support.

opentext™