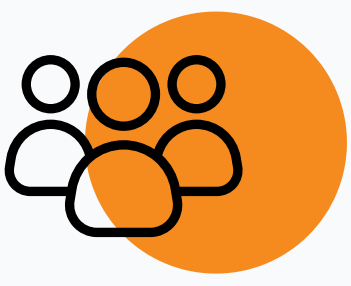
DEFEND YOUR BUSINESS

UNVEILING THE LATEST EMAIL SECURITY THREATS AND EXPERT TIPS

Of the 2.1 billion+ emails SYNAQ processed last year, close to half (41.9%) were quarantined or rejected. In the ever-evolving landscape of email security threats, it's crucial to stay informed and proactive in safeguarding your data:

BEST PRACTISES: COMBAT EMAIL THREATS WITH 4-P APPROACH:

PEOPLE



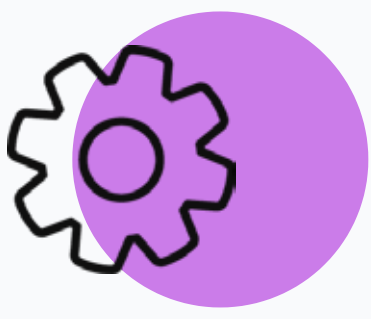
Educate and Train Employees on Email Security:

- Phishing Awareness Training: Identify suspicious emails
- Social Engineering Simulations: Test employee responses
- Reporting Procedures: Foster a culture of awareness

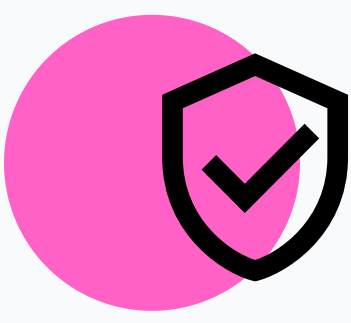
PROCESSES

Turn Email Security Best Practice's into Process:

- Strong Password Policies: Secure login credentials
- Encryption: Safeguard email content
- Regular Software Updates: Patch vulnerabilities



PLATFORMS



Implement Robust Email Authentication Measures:

- SPF, DKIM, and DMARC: Enhance email authentication
- Identity Threat Protection: Reduce the risk of spoofing with SPF verification, bypass protection, domain anti-spoof and executive fraud protection
- Effective SPAM Filters: Block suspicious incoming messages, links and attachments with advanced SPAM and URL threat detection and 100% virus protection

PROACTIVE

Get Proactive Monitoring and Incident Response

- Real-Time Email Monitoring: Detect anomalies
- Incident Response Plan: Establish steps to recover from breaches
- Threat Intelligence: Investigate incidents and gather evidence

HOW TO CHOOSE THE RIGHT EMAIL SECURITY PARTNER

Service Level Agreements (SLAs)

Understanding Security Commitments and Support

Look for a provider who guarantees 100% virus protection, and 100% punitive phishing protection against leading banks in South Africa. Consider value added services like training and support – and whether provider's local footprints and infrastructure can support those services in a way that makes sense given your business' needs.

Privacy and Compliance

Ensuring Regulatory Compliance in Email Communications

A breach in data-privacy legislation can be as costly as a cyberthreat data breach. Consider where you house your mailbox data and whether your hosting and email security provider is well-versed in (and more importantly, compliant with) relevant, localised legislation

Security Features

Encryption, Data Protection, and Anti-Malware Measures

Your provider should meet basic security requirements including domain authentication (SPF, DKIM, and DMARC), spam detection, virus protection, and Identity Threat Protection (ITP)

Remember, email security is not a luxury but a necessity. Prioritising and investing in email security today will go a long way in fortifying the defences of your business tomorrow and in the future. Stay vigilant, stay proactive, and stay secure in the face of evolving email security threats. Contact us to find out more.