SYNAQ

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:

WHAT TO LOOK OUT FOR IN EMAIL-BASED CYBERATTACKS IN 2023:

BUSINESS EMAIL COMPROMISE

WHAT?

Cybercriminals impersonate high-ranking executives or trusted vendors tricking employees into transferring funds or sensitive data.

HOW TO PROACTIVELY COMBAT

PLATFORM
Email security software including enhanced domain authentication (SPF, DKIM, and DMARC), SPF verification, bypass protection, domain anti-spoof and executive fraud protection.

PROCESS
Strict approval procedures for financial transactions.

PEOPLE
Train employees to identify BEC threats.

EXAMPLES

Spoofing (e.g. Executive Fraud; Vendor Email Compromise)

HOW TO SPOT

Unexplained urgency

Last minute changes in payment instructions

Refusal to communicate via telephone or in person

Unusual / generic greetings

PHISHING

WHAT?

A form of social engineering where Cybercriminals deceive people into revealing sensitive information or installing malware such as ransomware.

HOW TO PROACTIVELY COMBAT

PLATFORM
Email security software including Spam filters, anti-phishing technologies like ITP, phishing protection, antivirus, and LinkShield.

PROCESS
Adopt a Privacy-First approach to data management.

PEOPLE
Train employees to identify Phishing threats.

EXAMPLES

Spearphishing; whaling

HOW TO SPOT

Urgent action demands

Poor grammar and spelling

Requests to update login credentials, payment information or sensitive data

Offers that are too good to be true, or prizes for competitions you never entered

Threats to discontinue service.

RANSOMWARE

WHAT?

Cybercriminals use this malicious software, often delivered via phishing or BEC emails, to take control of critical business systems, encrypt data, and demand payments in exchange for restoring access.

HOW TO PROACTIVELY COMBAT

PLATFORM
Email security software including Anti malware threat detection and 100% virus protection.

PROCESS
Limit access to sensitive data by user and platform, robust backups network segmentation and regular security assessments.

PEOPLE
Instil a privacy first mindset and train employees to identify email threats.

EXAMPLES

BitPaymer. Cryptolocker, DarkSide, Dharma

HOW TO SPOT

Phishing or BEC emails

Suspicious attachments

TIPS TO THWART ATTACKERS

Check the sender email address, especially when using a mobile device.

Hover over any links before you click on them. If the URL of the link doesn't match the description, do not click the link.

Look out for spelling mistakes in hyperlinks.

Never contact the sender through the information provided in the email.

Report the email to the impersonated sender and to your IT department.

Do not click links or download attachments.

Delete the email.