SYNAQ

Do Your Part #BeCyberSmart

THE **A - Z** OF CYBER SECURITY AWARENESS FOR EMAIL

ANTI-VIRUS

Viruses can be transmitted in a variety of ways and have the ability to compromise sensitive information, destroy data, harm hardware and waste critical business time and resources. As part of a proactive and comprehensive security strategy, an effective email antivirus should be utilised to scan emails and attachments, isolate the affected emails and block them.

BRUTE FORCE ATTACKS

A brute-force attack is a trial-and-error method that obtains private user information (including login credentials, passwords and encryption keys) to gain unauthorised access to applications, networks, websites or email accounts. To mitigate these attacks, it is recommended that users increase password complexity or use passphrases and utilise services that proactively identify and protect against these attempts.

CYBERSECURITY

The strategy, solutions, policies and processes put in place to holistically safeguard confidential business information by protecting computers, cloud system applications, networks, programs and data from unauthorised access or hacking. We recommend working with cybersecurity specialists and putting solutions in place to protect your business from the evolving threat landscape.

DATA BREACH

An incident where information has been accessed or stolen from a system without the user or owner's permission or authorisation. Working with trusted and reliable security specialists who are POPI/GDPR-compliant will ensure that your valuable business information is safeguarded.

ENCRYPTION

Encrypting your email communication chain from end user to end user will prevent unauthorised users on the network from intercepting and capturing your login credentials or snooping on any email messages you send or receive. Does your existing email security solution encrypt each part of this chain effectively?

FILELESS ATTACKS

This type of attack often uses social engineering to get users to click on a link or an attachment in a phishing email. The fileless malware then infiltrates your machine's applications or operating system to initiate malicious processes. Email security solutions that protect users from URL-based phishing, ransomware and malware attacks, like SYNAQ LinkShield, should be utilised to protect your business.

GRAYWARE

Unwanted applications and software that can affect the performance of your computer and introduce the risk of the entry of more malicious threats. While not as malicious as conventional malware, it still poses a danger. So it is important for effective email security services to have comprehensive antivirus and protection from link-based threats. SYNAQ LinkShield will protect you from these applications.

HONEYPOT

A decoy system or network that serves to attract potential attackers to expose system vulnerabilities. At SYNAQ, we use honeypots to consistently train and update anti-spam and heuristics checks to ensure that our email security solutions are always up to date and can provide real-time email threat protection.

IDENTITY THEFT (SPOOFING)

Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they know or can trust. Users will then make themselves vulnerable by taking risky actions including clicking on malicious links, opening malware attachments or providing sensitive data. Protect your business using solutions that offer real-time antivirus protection and protection from link-based threats. SYNAQ has solutions to combat these risks including LinkShield and Identity Threat Protection, a toolset specifically designed to protect against spoofing.

JBOH (JAVASCRIPT-BINDING-OVER-HTTP)

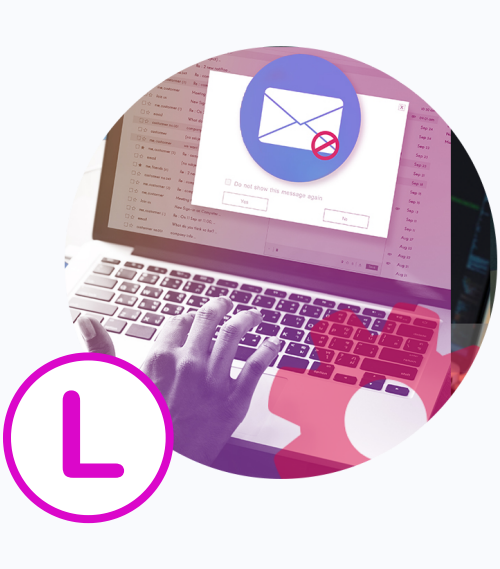
This is a type of mobile device attack in which compromised or malicious apps are used by attackers to initiate the execution of arbitrary code. JBOH attacks can be used to perform actions like mailing pre-crafted malicious emails to any designated recipient from the compromised device.

KILL CHAIN

Describes the stages of a cyberattack. In most attacks, there are four main stages:

1. Survey – The scouting of potential vulnerabilities for the cyberattack.
2. Delivery – The process of sending the attack hoping to breach the system.
3. Breach – When the system's defences are overpowered.
4. Attack – The stage where the damage is perpetrated.

Using a comprehensive set of layered email security solutions is key in protecting your business at all stages of the kill chain.



LINK-BASED THREATS

These are malicious attacks that originate from clicking on a link/URL. Protect your business email from URL based phishing, ransomware and malware attacks by using the SYNAQ LinkShield Service.

MALWARE

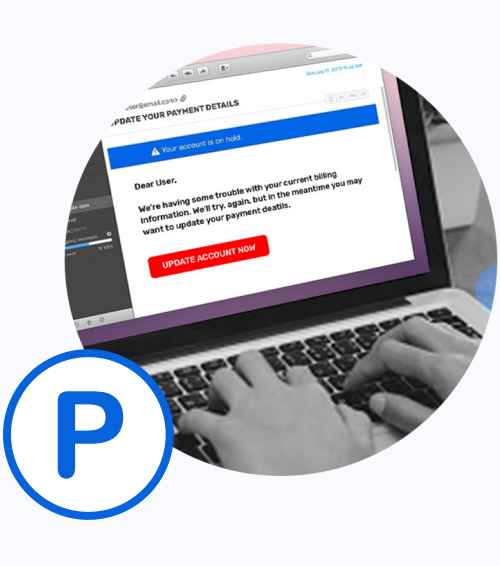
Malicious software designed to disrupt, damage or gain unauthorised access to a computer system. We recommend a comprehensive email security solution with effective antivirus and anti-spam heuristic checks to protect your valuable business data to ensure real-time email protection.

NETWORK RESILIENCE

As organisations add layers of complexity to networks, they often create more vulnerabilities, and they must consider network resilience at every stage of development. The recent Covid-19 pandemic also resulted in associated cyberattacks that require increased protection. There is a higher premium than ever on secure remote access and network resilience to ensure business continuity. Businesses must choose providers that frequently run vulnerability testing and implement comprehensive protection measures to ensure their survival.

OPPORTUNISTIC/ UNTARGETED ATTACKS

Cyberattacks are predominantly opportunistic. Cybercriminals diligently conduct broad scans of business environments, looking for vulnerabilities to exploit. Cybersecurity strategies will vary depending on the business context and the environment and technologies where they operate. But to avoid cyberattacks or minimise the damage they cause, consistent user education and awareness training and effective security solutions and applications that are well managed and updated should be a standard consideration. Don't leave your business exposed.



PHISHING

This is the fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information. Since 96% of phishing attacks arrive via email, we recommend a combination of solutions including Identity Threat Protection, anti-phishing heuristics protection and user awareness training to effectively identify and mitigate phishing attacks.

QUESTION

Be vigilant and question suspicious emails and anything that could affect cybersecurity in your organisation. Remember to:

- Look for clues of phishing such as spelling and grammar errors, even in emails supposedly from trusted sources.
- Be extra careful of emails that contain links and attachments, especially if they end in .exe, .cab, .htm, or .jar. Use multi-factor authentication to add an extra step in the verification process.
- Use encryption to convey especially sensitive information.
- Corroborate unusual claims or instructions received via email with a trusted information source.
- Be especially wary of emails that urge immediate action and use phrases like "Act now!"

  User awareness training on an ongoing basis is key. Contact SYNAQ if you notice any of these

RANSOMWARE

Ransomware is malicious software designed to block access to a computer system until a sum of money is paid. It is predominantly transmitted via email. Ensure you have a complete line of secure email defence which includes effective anti-spam and antivirus services.

SPAM

Unsolicited messages that are usually sent to a large number of users with the intention of introducing spyware, phishing opportunities, and the spread of malware. Protect your business from the possibility of these threats becoming a reality by using an email service that includes effective anti-spam and antivirus capabilities.

TWO-FACTOR AUTHENTICATION

An authentication method that requires two separate, distinct forms of identification to access something. It adds an additional layer of security, making it harder for cybercriminals to breach and gain access to your confidential systems and data. Since humans still present the weakest link in the security chain, we recommend using this method for as many systems and applications as possible.

UNAUTHORISED DISCLOSURE

Your organisation's insiders are an often-overlooked threat to its security. You could unwittingly create opportunities for serious data breaches by forgetting to revoke system access to a dismissed employee, granting third parties excessive access to your confidential data, or failing to adequately educate your staff about their role in cyberattacks. Internal security policies, processes and legal and compliance measures will aid to minimise unauthorised disclosure of critical business data.

VIRUS

Malicious code that can be transmitted via email in an attachment or link. Once accessed, it can spread across multiple devices, corrupt systems and destroy data. Your email security service should include effective antivirus and related heuristic solutions to prevent your business from falling prey to a virus.

WHALING AND SPEAR PHISHING

There are numerous categories of phishing, the most prominent of which are whaling and spear phishing. The difference between whaling and spear phishing is that whaling exclusively targets high-ranking individuals within an organisation (C-suite executives), while spear phishing will focus on lower-ranking employees. Utilising services like SYNAQ's Identity Threat Protection and anti-phishing heuristics, coupled with consistent user awareness training, will aid in protecting your business from these types of attacks.

X-PERT ADVICE

Why should you deal with security specialists? Experts can find out exactly what is best for your organisation by running security testing to identify key vulnerabilities or gaps in the environment. You need security providers who can protect the different aspects of your company.

YOU

Approximately 95% of cybersecurity breaches are caused by human error, and that's the reason for Cybersecurity Awareness Month's global theme, "Do Your Part #BeCyberSmart". Defending against social engineering attacks like phishing, spam and URL-based threats should be a continuous security education and awareness exercise. This will ensure that organisations can broaden their understanding of common threats and methods by sharing current and relevant use cases so that employees can learn to identify, mitigate and report these attempts.

ZERO-DAY VULNERABILITIES

Recently discovered vulnerabilities (or bugs) not yet known to vendors or antivirus organisations that hackers can exploit. Ensure you have a comprehensive arsenal of email security tools with heuristics to identify trends, formats and key phrases that can detect malicious emails. Using an email security provider that utilises multiple antivirus provider feeds will ensure that these vulnerabilities are caught early and proactively mitigated.