OneCollab

INTRODUCTION TO **CYBER SECURITY FOR BUSINESSES**

www.onecollab.co.uk

@onecollablimited
+44 20 8126 8620
info@onecollab.co.uk

Introduction

Welcome to our brief guide on business cyber security. This resource is designed as a strategic playbook, simplifying the complexities of safeguarding your digital assets for both seasoned entrepreneurs and those in the early stages of their business journey.

What is Cyber Security?

Cyber security entails protecting computer systems and networks from breaches, malfunctions, and digital attacks to safeguard data confidentiality, integrity, and availability. It actively counters threats like hacking, malware, and unauthorised access to ensure the security of digital assets and uninterrupted business operations.

Why is it Important?

By 2025, global cybercrime costs are projected to reach **$10.5 trillion** annually[1]. As cyber threats increasingly target individuals within organisations, the role of cyber security is pivotal in safeguarding corporate integrity. Enhancing cyber security practices and understanding potential threats are crucial steps to fortify defences. It's essential to recognise that cyber security is a collective responsibility, requiring vigilance and prompt reporting of any suspicious activity within the organisation.

Types of Cyber-Attacks

A cyber-attack is an intentional action to compromise a computer or its components, aiming to alter, destroy, pilfer data, or exploit and damage a network.

A few examples of cyber attacks are;

- Phishing Attacks
- Ransomware Attacks
- Malware Attacks

[1] Esentire Official Crime Report 2023

Phishing Attacks

What is Phishing in Cyber Security?

In the business realm, a phishing attack represents a form of social engineering where attackers aim to manipulate employees into taking detrimental actions.

Typically, these attackers send deceptive communications that convincingly mimic trusted and authentic sources within the business environment. These communications frequently incorporate links leading to deceptive websites, tricking individuals into revealing sensitive information or unknowingly downloading malware.

Crucially, victims within a business may not promptly recognise that they have fallen prey to a phishing attack. This lack of immediate awareness allows attackers to extend their reach within the organisation without arousing suspicion of malicious activity.

Remaining vigilant against phishing attempts is paramount for businesses, given that they persist as a prevalent and continually evolving cyber security threat with potentially severe consequences for organisational security.

Statistic

Phishing stands out as the primary method of email attacks, making up

39.6% of all email threats

[2] Hornets Security Cyber Security Report 2024

Guidelines for Spotting Phishing Attacks

Amidst ongoing phishing threats to businesses, cultivating awareness of risks is vital. Here are concise guidelines to spot and mitigate phishing risks in your business:

Verify Sender Identities

Exercise caution with emails from unfamiliar sources. Verify sender identities, especially for urgent requests or sensitive information.

Think Before You Click

Hover over email links to preview the URL; avoid clicking if it seems unrelated to the sender or appears suspicious.

Scrutinise Email Content

Closely scrutinise email language and content for errors or unusual requests, as phishing often involves such elements.

Examine Email Addresses

Carefully inspect the sender's email address for subtle variations or misspellings, as phishers often mimic legitimate addresses.

Beware of Urgent Requests

Beware of phishing emails inducing urgency, pressuring quick actions, and threatening negative consequences.

Educate Employees

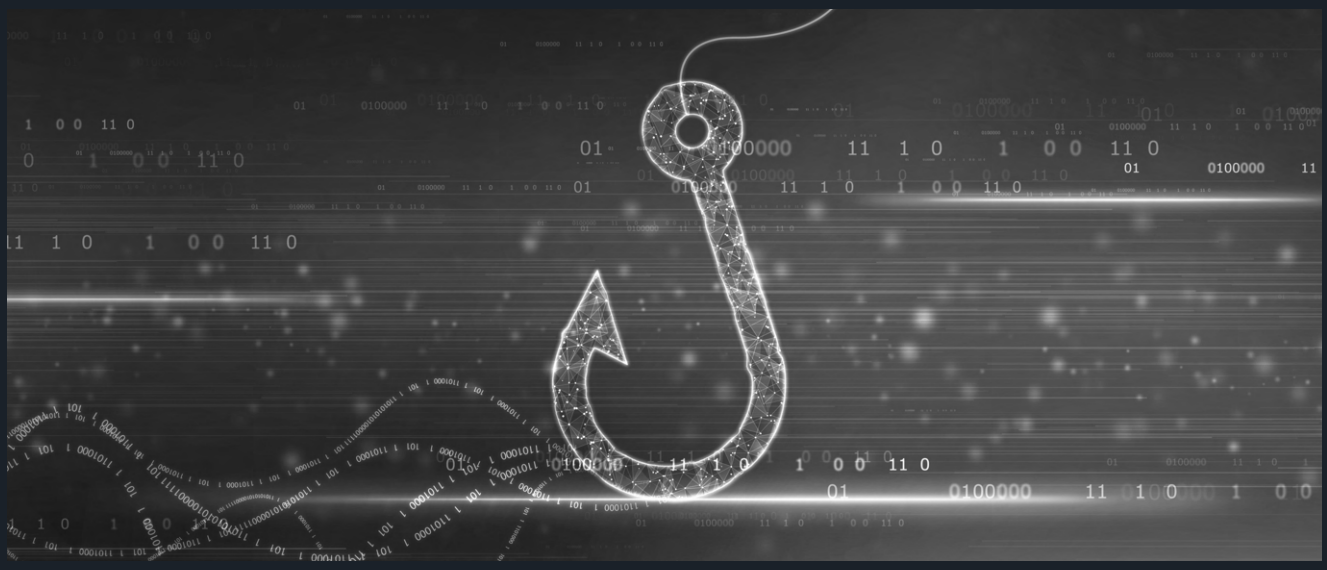
Train employees regularly to recognise phishing threats and encourage prompt reporting of any suspicious emails.

Enable Multi-Factor Authentication (MFA)

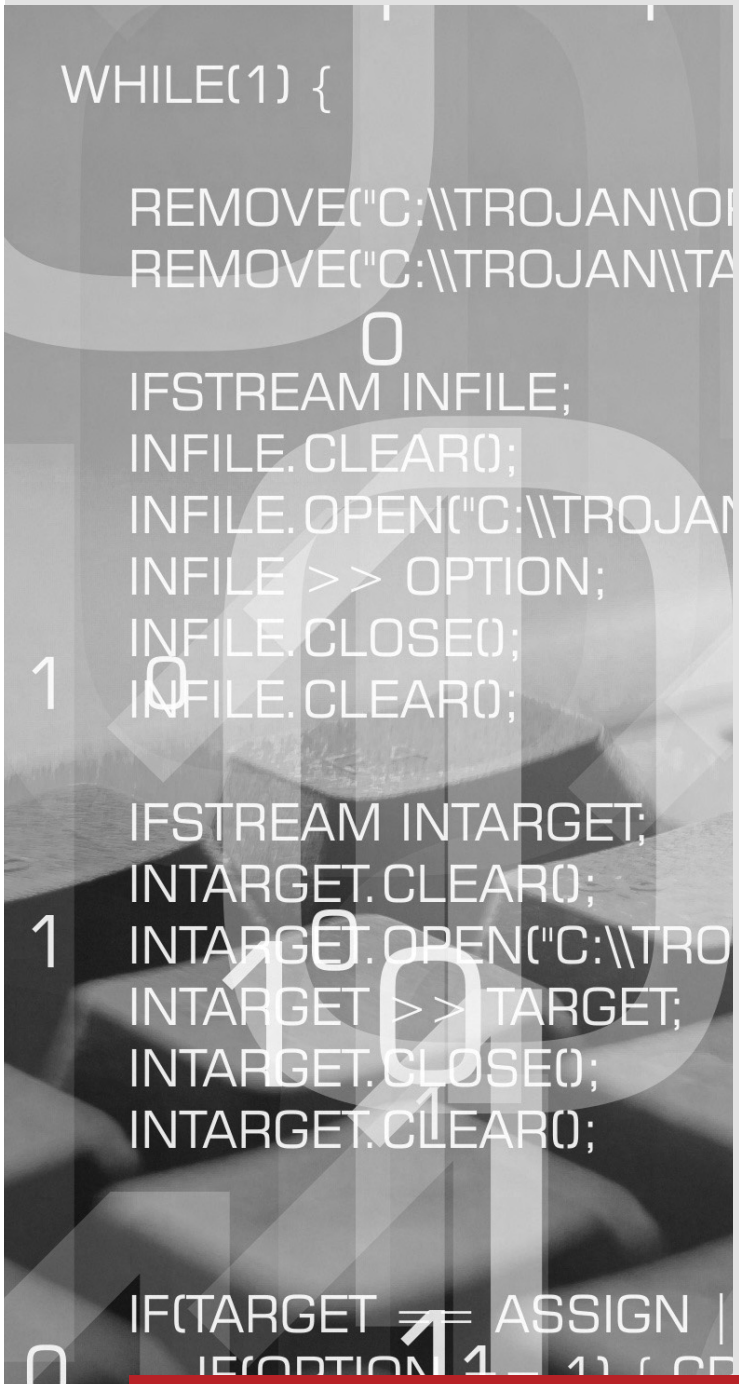
This adds an extra layer of security, making it harder for attackers to gain unauthorised access, even with compromised login credentials.

Use Advanced Email Security Solutions

Use advanced email security solutions to detect and filter out phishing attempts, bolstering overall cyber security defences.



Stay alert, keep up-to-date on phishing techniques, and foster a cyber security culture to defend against evolving cyber threats.



Ransomware

What is Ransomware in Cyber Security?

Ransomware, a malicious software, encrypts a user's files, rendering them inaccessible. Perpetrators demand a ransom, usually in cryptocurrency, for the decryption key.

This insidious malware often infiltrates through email attachments, exploiting unaddressed vulnerabilities in the system.

Operating covertly, ransomware makes detection challenging until damage is done. Its impact can extend by denying access to multiple computers or compromising central servers crucial for business operations. According to Statista, a staggering **72.7% of all organisations globally fell victim to a ransomware attack in 2023**[3].

To combat this threat, robust cyber security measures, including regular updates and employee training, are crucial for prevention.

Should I Pay The Ransom?

Paying a ransom can cost millions, and there's no guarantee that hackers will release data—only **60% regain access after the initial payment**[4].

The risks extend to contravening insurance policies, potential criminal liabilities, and penalties. Moreover, it increases vulnerability for future attacks, as cybercriminals learn about systems and exploit weaknesses. Funding criminal activities and reinforcing a culture of cybercrime make paying ransoms an unfavorable option.

Instead, the best solution lies in ransomware-ready backups, providing a resilient, high-security defence against attacks and reducing downtime costs.

[3] Statista Businesses Ransomware Attack Rate

[4] TechTarget 'Should Companies Pay Ransomware and is it Illegal to?

Guidelines for Preventing Ransomware Attacks

In the ever-evolving landscape of cyber threats, businesses face the looming risk of ransomware attacks. Here is essential guidance to fortify your cyber security defences and mitigate the impact of potential incidents:

Backup Critical Data

Backup crucial data regularly to offline or secure cloud storage for unaffected copies in case of a ransomware attack.

User Awareness Training

Educate employees to spot ransomware threats, avoid unknown links, and don't open unexpected attachments to minimise risk.

Implement Robust Security Measures

Use advanced antivirus and anti-malware software to enhance the overall cyber security posture of your systems.

Access Control and Least Privilege

Restrict user permissions & access to the minimum required for job functions. Limiting privileges reduces the potential impact of ransomware.

Network Segmentation

Segmenting your network and isolating critical systems helps contain the spread of ransomware, preventing rapid attack expansion.

Regularly Update Software

Ensure timely protection by keeping operating systems and software up-to-date, using automated updates to patch vulnerabilities.

Incident Response (IR) Plan

Develop and regularly test an IR plan, ensuring employees are familiar with proper procedures for a ransomware attack.

Enable Multi-Factor Authentication (MFA)

Implement MFA for sensitive system access, adding an extra layer of security to prevent unauthorised access.

Regular Security Audits

Regularly audit security to assess vulnerabilities and ensure effectiveness against evolving ransomware tactics.

Communication Protocols

Establish clear communication protocols for ransomware incidents, both internally and externally, to manage the situation effectively.

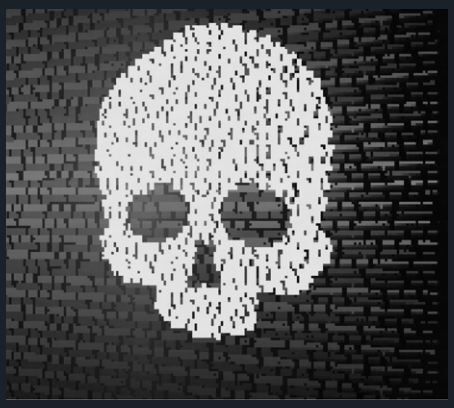
Collaborate with Cyber Security Experts

Build ties with cyber security experts or firms for valuable expertise in proactively identifying and mitigating potential threats.

Legal and Regulatory Compliance

Comply with relevant legal requirements for handling ransomware incidents, including reporting and data protection laws.

Malware Attacks



What is Malware in Cyber Security?

Malware, short for malicious software, includes various types of harmful software designed to compromise, damage, or exploit computer systems. It can manifest as viruses, worms, spyware, Trojans, ransomware, and more.

Malware in Numbers

According to the AV-TEST Institute, there are over **1 billion malware programs** installed worldwide, with **560,000 new** pieces detected each day[5]. This staggering figure emphasises the urgent need for robust cyber security measures to combat the pervasive and evolving threat posed by malware.

What is the Intent of Malware?

Malware is crafted as malicious software to infiltrate or disrupt computer networks. Its objective is to wreak havoc, pilfer information, or acquire resources for financial gain or deliberate sabotage.

Intelligence and Intrusion

Malicious software excels at covertly infiltrating systems to extract sensitive information, compromising the security and privacy of businesses by stealing emails, strategic plans, passwords, and other critical data.

Financial Gain

Malware often targets financial gain, with cybercriminals trading stolen intellectual property, including proprietary and sensitive data, on the dark web. This underground marketplace fuels the cybercriminal ecosystem.

Disruption and Extortion

Beyond extracting information, malware disrupts networks and computers, severely impacting operational efficiency. When the goal is financial gain, malware transforms into ransomware, holding computers hostage and demanding payment for release.

[5]AV-TEST 'Malware Statistics'

Guidelines for Preventing Malware Attacks

In the relentless landscape of cyber threats, defending against malware attacks is paramount. Here's essential guidance to fortify your cyber security defences and mitigate the impact of potential malware incidents:

Implement Antivirus

Use advanced antivirus and anti-malware software to detect and neutralise malware threats in real-time.

Regularly Update Software

Keep all security software up-to-date to ensure it is equipped to combat the latest malware variants effectively.

Employee Least Privilege Principle

Enforce the principle of least privilege for user accounts, limiting access rights to the minimum necessary for job functions.

Employee Training on Cyber Hygiene

Educate employees on cyber security, stressing the need to steer clear of suspicious links, email attachments, & software downloads.

Network Segmentation

Segment your network to limit the lateral movement of malware. This containment strategy helps prevent widespread infection.

Backup Critical Data

Regularly back up critical data to offline or secure cloud storage to mitigate the impact of data loss in the event of a malware attack.

Implement Email Filtering

Employ robust email filtering solutions to screen and block malicious emails before they reach employees' inboxes.

Endpoint Security

Enhance endpoint security with intrusion detection systems, firewalls, and endpoint detection and response (EDR) software.

User Behavior Analytics

Implement user behavior analytics tools to detect anomalous activities that may indicate a malware infection.

Regular Security Audits

Regularly audit security to identify vulnerabilities and assess measures against evolving malware threats.

Implement Application Whitelisting

Restrict the execution of applications to an approved list to prevent unauthorised software and malware.

Secure Web Browsing

Encourage cautious browsing and enhance defences with robust web filters to block potentially malicious websites.

Boldly adopting these proactive measures and maintaining an unyielding vigilance can empower organisations to significantly diminish the risk and impact of malware attacks on their cyber security infrastructure.

What Else Can I Do to Keepy My Business Safe from a Cyber-Attacks?

Uncover additional layers of protection beyond the essentials to secure your business against a diverse range of cyber threats:

Secure Remote Work Practices

Implement secure remote work measures, utilising VPNs and secure communication tools to safeguard against cyber threats.

Third-Party Risk Management

Thoroughly assess third-party vendors to ensure robust cyber security standards, minimising external connection vulnerabilities.

Secure Disposal of Old Devices

Establish secure protocols for disposing of old devices, ensuring thorough data wiping or destruction to prevent unauthorised access.

Security Information and Event Management (SIEM)

Employ SIEM solutions for real-time analysis of security event data to proactively detect and respond to potential cyber threats.

Advanced Network Security Measures

Implement intrusion prevention systems (IPS) and network segmentation, to detect and contain potential cyber threats.

Proactive Security Monitoring

Establish proactive security monitoring practices to identify anomalous activities and potential security incidents in real-time.

Encryption

Implement intrusion prevention systems (IPS) and network segmentation, to detect and contain potential cyber threats.

Data Loss Prevention (DLP)

Implement DLP solutions to control and prevent unauthorised data transfer, ensuring complete data flow control in your business.

How We Can Help

In the dynamic field of cyber security, we empower your business with bespoke solutions, including cutting-edge technologies, proactive defence measures, and advanced threat detection for a resilient security posture.

From personalised consultations to continuous monitoring, 24/7 support, and strategic planning, our services ensure enhanced protection for your business.

Contact us today at info@onecollab.co.uk to embark on a journey of enhanced protection and digital resilience.

Find Out More:
www.onecollab.co.uk

@onecollablimited
+44 20 8126 8620
info@onecollab.co.uk

INTRODUCTION TO
CYBER SECURITY
FOR BUSINESSES