CASE STUDY

Cyber Security for SMEs: **Providing security layers** for Prime Clean

PRIME CLEAN

TECHARY

CLIENT

Primarily offering services across London and the Home Counties, Prime Clean operates across a wide range of business sectors, including professional services, education, hospitality, retail and the public sectors.

REQUIREMENT

Although based in London, Prime Clean staff often work “on-the-move” between client premises across the UK. This usually means that users are communicating on mobile devices, e-mailing and working on documents using Office 365. Having used Office 365 for over five years, the business adopted the cloud-based solution early on and has since benefitted from increased flexibility and easy access to resources in a mobile working environment. However, at the start of this year users began to report an increasing amount of phishing attempts, with various users receiving impersonation e-mails.

Support Projects Procurement Resources

SOLUTION

Working with Prime Clean, our Information security team identified current exposures within the system architecture and sought out to implement additional security layers to remediate any live phishing attempts as well as provide a future safeguard for the agile workforce. We deployed 2-factor authentication for all users within the business (previously this was only enforced at management level). This immediately provided a first line of defence against the live threats.

Our partnership with Barracuda enables us to run live scans of the Office 365 environment in order to identify and revoke all live threats within live mailboxes. We were able to conduct and run the scan and stop and remediate all live threats within 4 working hours. Subsequently, we used Barracuda’s 365 protection to provide a comprehensive security protection layer inclusive of:

- Email security and threat protection
- Archiving
- Point-in-time backup
- Continuity layer

E: info@techary.com **W:** techary.com

This layer provides additional security, automatically quarantining e-mails that the AI engine believes to be suspicious. Users are then provided with updates of the held mails, with the ability to release, whitelist or blacklist the recipient. The system develops intelligence in accordance with the user input, so within around two weeks, 99% of held mails are fraudulent or unwanted. We also implemented some simple additional security layers, such as message headers that alert users to any external mails. The aim of these is to remove impersonation attempts from external domains. We have also enabled DKIM and DMARC on the company’s domain name, with reports reviewed by our SOC daily.

We wanted to ensure that the user-base were not only kept up-to-date with the changes that were being made throughout the process, but also understood how and why we were making the changes.

USER AWARENESS

We wanted to ensure that the user-base were not only kept up-to-date with the changes that were being made throughout the process, but also understood how and why we were making the changes

User awareness still remains the best line of defence against cyber vulnerabilities, so keeping everyone up-to-date and aware of the ways in which attacks can be performed, along with the security layers that exist within the business, will help to increase vigilance within the workforce.

RESULT

Prime Clean are now looking to adopt the Cyber Essentials certification, which will only help them to continue to grow their business, with their customers secure in the knowledge of their supplier’s investment into its Cyber Security protection.