

MONTHLY SECURITY BRIEFING

Practical cyber awareness for safer everyday work



OVERVIEW

Monthly Security Briefing is a practical on-demand cyber awareness programme that helps staff recognise modern cyber risks and make safer everyday decisions. Delivered across 12 monthly mini-series, the training covers phishing, ransomware, account takeover, exposed data, AI-enabled scams, remote working, sensitive information and incident reporting. Each mini-series ends with a short test to reinforce learning.

12 MONTHLY MINI-SERIES

1

Security Foundations

What cybersecurity protects, why attackers target organisations, and the value of data, money, access and trust.

7

Passwords & Access

Password security, MFA, credential stuffing, account takeover, passkeys, password managers and safe login routes.

2

Dark Web

The surface, deep and dark web, criminal marketplaces, access brokers, cryptocurrency and cybercrime-as-a-service.

8

Ransomware

Initial access, quiet movement, backup targeting, data theft, encryption, response, recovery and lessons learned.

3

Exposure & OSINT

Breached data, exposed personal information, public information, LinkedIn, websites, job adverts and AI-powered reconnaissance.

9

AI-Enabled Risk

AI-powered scams, deepfakes, voice cloning, prompt injection, malicious automation and safer AI use.

4

Phishing

Fake senders, suspicious links, fake login pages, spear phishing, AI-personalised phishing and safe verification habits.

10

Everywhere Work

Hybrid work, public Wi-Fi, VPNs, stolen devices, home Wi-Fi, IoT devices and secure remote working.

5

Warning Signs

Early signs of attack, suspicious emails, business email compromise, malware and ransomware indicators, and fast reporting.

11

Business Data

Where business data lives, sensitive information, approved systems, safe sharing and breach prevention.

6

Human Factor

Social engineering, authority, urgency, fear, curiosity, trust, overconfidence and pause-and-verify habits.

12

Scams & Deception

Messaging scams, social media scams, vishing, deepfake calls, multi-channel attacks, trusted process and reporting.

12 timed mini video series

practical everyday cyber awareness

clear documentary-style training