London Digital Security Centre

Overview

The London Digital Security Centre (The Centre) is a **not for profit** organisation founded by the Mayor of London as a joint venture with The Metropolitan Police and the City of London Police

The Centre is here **to help protect businesses**, primarily micro to medium sized businesses, **to operate in a secure digital environment.** The Centre works alongside the **National Fraud and Cyber Crime Reporting Centre (ActionFraud).**

The Centre takes its **advice and guidance from the National Cyber Security Centre**.

The Centre seeks to support businesses to **innovate and grow** through embracing digital opportunities.

The Centre aims to **reach the estimated one Million SMEs** operating in London through working in partnership with trade bodies, local authorities and policing.

Membership

The Centre has launched a **free membership scheme** for small and medium sized businesses.

Membership is free, and provides **each member with an initial assessment of their digital security needs** as part of the sign-up process. This assessment will be based on understanding how each business specifically operates in the digital world and each member will then receive complimentary services that will help to enrich their digital security.

Members receive **tailored support** for example access to timely advice, alerts regarding latest threats and vulnerabilities, as well as training and education programmes for staff to help enrich their digital security posture.

Membership involves a programme of activities that assesses each business's security risks, puts controls in place to mitigate these risks, tests the controls and then reassesses each businesses security posture.

The Centre is able to do this through use of a **security scorecard** product, and using methods such as phishing, smishing and social engineering.

Digital Security Clinics

The Centre holds Digital Security Clinics across London for members to discuss, on a one to one level, how best to operate in a secure digital environment.

These are free to attend and there is no requirement to be a member of the Centre.

Each clinic is advertised via **www.Londondsc.co.uk.**

Market Place

The purpose of the Market Place is to **provide affordable and appropriate products for an SME** to help enrich their digital security posture.

The MarketPlace provides members with access to business resilience products and services supplied by **market leading private sector organisations**.

The MarketPlace is accessible via **www.Londondsc.co.uk**

In The Community

Continuous programme of activities, targeting every borough in Greater London and the City of London.

The purpose of the in the Community work is to take **Digital Security to the High Street** and to provide small and medium sized businesses with visible support to **enrich their digital security posture**

As a result of this engagement, we are able to start building a picture of the current security posture of businesses operating in London. In effect, we are building an **evidence base of the vulnerabilities** that businesses in the London have to known criminal attacks.

All future in the Community events are advertised via **www.Londondsc.co.uk**

Partnership / Sponsorship

There are three levels of partnership:

- **Product Partner** – these are carefully selected companies that offer market-leading solutions on our MarketPlace

- **Alliance Partner** – Our Alliance Partners are a small number of organisations who have helped build its capability and our thinking, they are invested in helping us taking our ambitions forward and their organisations embrace the Centre's mission. They are instrumental in helping us provide complimentary

services to our members and have helped us to identify appropriate paid for service and product offerings. They have also supported our events through sponsorship.

- **Strategic Partner** – The Strategic Partner Programme is designed to support the Centre meet its mission and goals. It has been specifically designed to create partnerships with some of the UK leading businesses and organisations, working closely with the Centre through a combination of activity to reach, inform and have an evidence based positive impact on the digital footprint of the SME community.

The Centre delivers a number of **free events** aimed at enriching a business' security posture. We seek sponsorship to help deliver these.

Organisations interested in partnering, or sponsoring, the Centre can contact us via **www.Londondsc.co.uk**

Key Stats

- Estimated one million SMEs operating in London
- 1000+ businesses in London report being the victim of a cybercrime or fraud each month to ActionFraud
- In the Community engagements (242 businesses) have identified:
  - 56% are running outdated software
  - 24% do not have anti-virus on their machines
  - 69% do not have policies re use of bring your own device
  - 74% do not use encryption
  - 95% do no use DMARC
- Verizon data breaches report 2017 states:
  - 81 percent of hacking-related breaches leveraged either stolen and/or weak passwords
- DCMS Report April 2017
  - Just under half (46%) of all businesses identified at least one breach or attack in the last year:
    - 45% of micro / small businesses
  - The most common types of breaches related to:
    - staff receiving fraudulent emails (72% of those who identified a breach or attack)
    - viruses and malware (33%)
    - people impersonating the organisation online (27%)
    - ransomware (17%)

Top Tips

- Install the latest software and app updates; they contain vital security upgrades which help protect against viruses and hackers
- Use strong and separate passwords for your key accounts, including email and online banking and use three random words to make a strong and memorable password
- Provide staff with access to simple, freely-available cyber security training
- Back up essential data at regular intervals
- Conduct a cyber security risk assessment for your business
- Seek accreditation through the Government-endorsed 'Cyber Essentials' scheme
- Never disclose security details such as passwords or PINs
- Don't assume an email, text or call is authentic; just because someone knows your basic details, it doesn't mean they are genuine
- Ensure that administration accounts are not used for routine activities such as browsing and emailing
- Deploy DMARC and SPF.