



Press Release

12 October 2017

How London SMEs can Improve their Digital Security for Free

Ahead of its briefing event at City Hall today with the Deputy Mayor for Business, Rajesh Agrawal and the Capital's Chief Digital Officer, Theo Blackwell, the London Digital Security Centre releases its first insights into Member data and identifies how SME's can increase their digital security for free.

London, UK - New member data released today by the [London Digital Security Centre](#) in support of European Cyber Security Month highlights that some London SMEs are struggling to understand which best practice digital security processes should be put in place to protect themselves online.

The information follows the recent announcement in The Telegraph on Sunday 8 October, from Ian Fleming, head of the intelligence monitoring service GCHQ, that the threat of cyber security to the UK is "as serious as terrorism".

Enabling SMEs to improve their existing cyber security protocols by identifying and implementing the appropriate controls is at the heart of the free membership offered by the Centre. The Centre's data

Issued by: Alison Page, Director of Communications for London Digital Security Centre. Tel: 07963 002065 for more information.

shows that not all London SMEs are aware of the simple digital security processes they can add to their business operations as currently:

1. 69% are running outdated software on their network
2. 74% do not have policies regarding use of bring your own device (BYOD)
3. 24.59% do not have anti-virus programmes on their machines
4. 69% do not use encryption software
5. 84.54% do not use digital signatures
6. 76.58% do not use DMARC (Domain-based Message Authentication, Reporting and Conformance, an email authentication, policy and reporting protocol).

“The London Digital Security Centre is today issuing a call to action to business communities across London to help them keep smaller businesses safe and to protect the back bone of London’s economy. It is estimated that there are one million SMEs operating in London and we are offering all of them free support and guidance to help them get the basics right to enrich their digital security.” reveals John Unsworth, the Centre’s Chief Executive.

He continues; *“If you hold data, you are a viable target - the Department for Digital, Culture, Media & Sport highlighted in April, that 45% of micro/small businesses have been the victims of successful data breaches or attacks over the past 12 months so the threat is particularly real and potentially devastating to small businesses. We are here to help London SMEs understand what makes a good security posture and what they can do to improve their existing security.”*

Issued by: Alison Page, Director of Communications for London Digital Security Centre. Tel: 07963 002065 for more information.

An initial assessment of each SME's digital security needs is undertaken as part of the Centre's sign-up process based on understanding how each business specifically operates in the digital world. Each member then receives complimentary advice, services and training that will help to keep them safe from fraudulent emails, viruses and malware, people impersonating the organisation online and ransomware.

Best practice advice on digital security for SMEs from the London Digital Security Centre includes:

1. Install the latest software and app updates; they contain vital security upgrades which help protect against viruses and hackers
2. 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
3. Provide staff with access to simple, freely-available cyber security training
4. Back up essential data at regular intervals
5. Conduct a cyber security risk assessment for your business
6. Seek accreditation through the Government-endorsed 'Cyber Essentials' scheme
7. Never disclose security details such as passwords or PINs
8. Don't assume an email, text or call is authentic; just because someone knows your basic details, it doesn't mean they are genuine
9. Ensure that administration accounts are not used for routine activities such as browsing and emailing
10. Deploy DMARC and SPF (Sender Policy Framework, validates a message's email domain).

Issued by: Alison Page, Director of Communications for London Digital Security Centre. Tel: 07963 002065 for more information.

October 2017 is European Cyber Security Month ([ECSM](#)) and this EU awareness campaign promotes cyber security among organisations and individuals and highlights the simple steps that can be taken to protect their data, whether personal, financial and/or professional.

For further information on the London Digital Security Centre please visit www.londondsc.co.uk or contact John Unsworth by email at: john.unsworth@londondsc.co.uk.

--- Ends ---

Note to editors:

The London Digital Security Centre is a not for profit organisation founded by the Mayor of London as a joint venture with the Metropolitan Police Service and the City of London Police. The Centre works alongside the National Fraud and Cyber Crime Reporting Centre (ActionFraud) to help prevent businesses being the victims of cybercrime.

The London Digital Security Centre provides free impartial advice and support to businesses to help improve their digital security and enable them to work in a secure online environment.

Website: www.londondsc.co.uk

Twitter: <https://twitter.com/LondonDSC>

Linked in: www.linkedin.com/company/london-digital-security-centre

Further Information Contact: John Unsworth, Chief Executive

Telephone: +44 (0) 7786 327520

Email: john.unsworth@londondsc.co.uk

Press Information Contact: Alison Page, Director of Communications

Telephone: +44 (0) 7963 002065

Email: a.page@londondsc.co.uk

Issued by: Alison Page, Director of Communications for London Digital Security Centre. Tel: 07963 002065 for more information.