



## **PCI Pal study reveals that Londoners are the biggest risk takers with their personal data security practices**

A consumer study that questions UK consumers' attitudes into their personal data sharing habits has revealed that people living in London are inclined to disclose more information about themselves on social media, compared to people living in other regions of the country.

The study by [PCI Pal®](#) found that Londoners are most likely to accept unsolicited friend requests, download and open unverified email attachments, as well as use public Wi-Fi networks to make purchases, pay a bill or check their bank accounts, compared to others.

In advance of the peak Black Friday and Christmas shopping seasons, the findings of the study also delves into peoples' attitudes regarding their personal data security practices and, overall, found the following trends:

- Despite many warnings, over a quarter (26%) of all respondents use the same password for multiple websites – with 49% of people from London agreeing to this, compared to just 16% in East Anglia. Almost half (46%) of those aged 35-44 admitted to using the same passwords for multiple sites.
- Despite the recent announcement that a new payment system is launching for Facebook, Instagram and WhatsApp, 69% of all respondents say they would not feel comfortable paying via a mobile app, SMS or web-chat. When looking at regions, this increases to 84% of those in the East, 82% in the South West and 78% in Yorkshire and the Humber.
- In contrast those from London said they feel either extremely (20%) or moderately (27%) comfortable with paying via a mobile app, SMS or web-chat.
- 56% of those in the North East and 55% of Londoners publish their full names on social media profiles; 38% of Londoners and 36% of those from the South East have their date of births publicly visible on social media; and 36% of Londoners openly publish their education history and 11% have shared their pets' names.
- 79% of all respondents say they never accept unsolicited friend requests on social media – although this figure increases to 90% of those from Yorkshire & Humber and 88% of those from

the North West of England who are more wary; in contrast 40% of Londoners said they have accepted unknown friend requests on social media.

- Over a third (38%) of Londoners have admitted to opening unverified links or downloading attachments for both work and personal accounts, however 94% of those in Yorkshire and Humber, and 91% of respondents in both the North West and the South West have said they have never done this.
- When considering activities undertaken via public Wi-Fi, 34% of Londoner's admitted to logging into emails with passwords, 31% have made purchases, 27% have checked their bank account and 26% have paid a bill. In comparison, almost three quarters (74%) of those in the West Midlands, East Midlands, the South West and Yorkshire and Humber have never attempted any of these activities using public Wi-Fi.
- All respondents are most likely to share the following information over the phone: name (71%), email address (57%) and home address (49%). 65% of respondents say they would only give this information if they called the person/organisation.
- 92% of respondents aged 65+ have never accepted unsolicited friend requests on social media
- 61% of respondents say that they either rarely or never check their credit scores.
- 69% of all respondents – and 78% of those in the North East – say they have never been the victim of a scam, breach or fraud that led to some of their money or data being taken without their knowledge. In contrast 41% of Londoners have been the victim of a scam, breach or fraud, in addition to 29% of those in the East Midlands.
- Face to face transactions remain the firm favourite, with 80% of people preferring to pay in person using a credit or debit card, closely followed by 79% of those wishing to pay in person, using cash.

Talking about the findings, Geoff Forsyth, CISO at PCI Pal said, "Despite the many warnings and many news stories relating to high profile data breaches, scams or hacks, there is still some way to go to educate people into the dos and don'ts of securing their personal data. Many continue to reveal their full names, dates of birth, employment history – even their pets' names – and this type of data may provide hackers with an unfair advantage, while making consumers unnecessarily vulnerable to potential data security risks.

"Our advice would be to lock-down your personal data wherever possible. Use password manager software to ensure a unique password for each website you visit – that way, if one site is compromised, the hackers cannot access your other accounts. Do not share sensitive information on

public Wi-Fi networks such as libraries and coffee shops. And, if shopping online or over the phone for Black Friday or Cyber Monday this year, make sure the website shows a security padlock and ask telephone advisors how they process card.”

For more information on PCI Pal visit [www.pcipal.com](http://www.pcipal.com), call +44 207 030 3770 to arrange a demonstration or follow PCI Pal on [Twitter](#).

ends

**Notes to Editors:**

- An online survey was conducted by Atomik Research among 1,000 adult respondents from the UK. The research fieldwork took place on 30<sup>th</sup> October. Atomik Research is an independent creative market research agency that employs MRS-certified researchers and abides to the MRS code.
- For more information, the full Risk Calculator report and statistics are available on request.

**About PCI Pal**

PCI Pal® is the specialist provider of secure payment solutions for contact centres and businesses taking Cardholder Not Present (CNP) payments. PCI Pal’s globally accessible cloud platform empowers organisations to take payments securely without bringing their environments into scope of PCI DSS and other card payment data security rules and regulations.

With the entire product portfolio served from PCI Pal’s cloud environment, integrations with existing telephony, payment, and desktop environments are simple and light-touch, ensuring no degradation of service while achieving security and compliance.

PCI Pal has offices in London, Ipswich (UK) and Charlotte NC (USA). For more information visit [www.pcipal.com](http://www.pcipal.com) or follow the team on Twitter: <https://twitter.com/PCIPAL>

**Editor’s Contact:**

Peppa Sheridan  
Peptalk Communications  
+ 44 (0)1787 313822  
[peppa@peptalkpr.co.uk](mailto:peppa@peptalkpr.co.uk)