Data & E-Media Security

TOPWOOD
STORAGE • SCANNING • SHREDDING

Identity theft is the fastest growing form of consumer fraud in the UK. The consequences for businesses are enormous both in terms of detect costs and potential damage to corporate reputation.

Identity Theft Facts

- The statistics, from 277 banks and businesses, show almost 173,000 recorded frauds in 2016 - the highest level since records began 13 years ago (according to bbc.oc.uk/news/uk 15.03.17)
- According to actionfraud.police.uk fraud losses to SMEs are estimated at a staggering £19billion a year
- Fraud costs £1000 per UK adult (source: National Fraud Authority www.bba.org.uk)
- Shockingly 78% of businesses make no effort to have a comprehensive policy with clear dos and don'ts fro employees to follow to help protect peoples identities http://www.stop-idfraud.co.uk/thefacts/business)

Identity Theft Prevention Tips

At home:

- ✓ Be careful when giving personal information, especially by telephone or online
- ✓ Use a locked mailbox
- ✓ Keep your personal documents in a locked box, secure storage area or personal safe
- ✓ Carry a minimal amount of personal information in your wallet
- ✓ Take receipts when leaving stores and restaurants
- ✓ Destroy envelopes and return address labels
- ✓ Check your credit report every year and report problems immediately
- ✓ Shred unwanted receipts, cheques, pre-approved credit applications and old tax returns

In the Workplace:

- ✓ Understand your company's privacy and document destruction policies:
  - Only collect essential data and obtain consent when you collect data
  - Limit access to sensitive data
  - Encrypt data networks, laptops, and remote access devices
  - Conduct employee background checks
  - Use locks, alarms and video cameras
  - Prepare a strategy to manage a security breach
- ✓ Ensure data is stored in a secure place and develop a DOCUMENT MANAGEMENT SYSTEM.
- ✓ Shred all sensitive documents and old files: business forms, customer data, letterhead, proprietary information, business cards, contact lists, receipts and financial reports

Conclusion

- Encourage your staff to consider their own personal security and the implications of having their personal details stolen
- Help them develop steps and protocol to prevent data breach
- Ask them to consider the impact of a data breach in the workplace
- Develop clear policies and guidance to help staff protect the data your business holds.