



Fraud is often assumed to be just a digital issue

Fraud is often thought mistakenly as just a digital issue, like a hacking incident. But it can take many forms including physical document exposure, which is just as dangerous and often overlooked.

Here are some of the ways in which you may be putting your business at risk:

Physical Document Exposure

-  **Unshredded paperwork:** Documents containing sensitive information e.g. invoices, contracts, medical records, employee files left in bins, desks or recycling can be stolen or misused.
-  **Improper disposal:** Tossing documents without secure destruction like shredding, opens the door to bin raiding and identity theft.

Insider Threats

-  Employees or contractors may misuse access to physical files, especially if there are no controls or tracking systems in place.

Social Engineering

-  Fraudsters may use physical documents to impersonate individuals or businesses, gaining access to systems or financial resources.

Hybrid Attacks

-  Physical documents can be used to support digital fraud for example, using a printed bank statement to bypass identity verification in online scams.

How you can help prevent fraud beyond the digital threats:

Conduct a Data Security Assessment

-  Review how confidential information is stored, accessed and disposed, both digitally and physically.
-  Identify vulnerabilities in document handling, storage areas and disposal processes.
-  Use this assessment to update policies and train staff accordingly.

Enforce a Clean Desk Policy

-  Require employees to clear desks of all sensitive documents at the end of the day.
-  Lock away paperwork, USB drives and devices when not in use.
-  This reduces the risk of accidental exposure or theft, especially in shared or open-plan offices.

Train Staff on Handling Confidential Information

-  Ensure all employees understand what constitutes confidential data.
-  Provide clear guidelines on how to store, share and dispose of sensitive documents.
-  Include real-world examples of physical fraud to highlight the risks.

Adopt a Shred-It-All Policy

-  If in doubt, shred it. This removes the guesswork and ensures no sensitive documents fall into the wrong hands.
-  Promote this policy as a simple, effective way to protect both customer and business data.
-  Appoint someone in your company to monitor the Shred-it All process e.g., checking printers for stray documents.

For more information, visit shredit.co.uk or call 0800 197 1164.

We protect what matters.