# Shred Station's Fraud Awareness Guide for Businesses


www.shredstation.co.uk

# Contents

While some businesses are targeted more than others, no business or charity is ever totally invulnerable to the risk of fraud. By implementing security measures and training your teams on the risks and how to detect fraud early, your business stands the best chance against fraudsters both externally and within company walls.

This Fraud Awareness Guide for Businesses will cover a number of areas, including the most common types of fraud to look out for, and how to minimise the risks.

# Common types of fraud

The best way businesses can protect themselves from the risk of fraud is to have efficient data and financial safeguards in place. This can include everything from robust cyber security to timely data destruction and staff training.

There are countless types of fraud, but once employees know the signs to look out for, fraud instances can be easier to spot and therefore easier to avoid.

**In this document we'll be covering:**

- Phishing emails
- Employee fraud
- Invoice fraud
- Money laundering
- IT attacks
- Espionage
- Procurement fraud
- CEO fraud and social engineering.

Fraudsters can use highly sophisticated techniques to go unnoticed when targeting businesses, so making all employees aware of these techniques and ways to combat them is fundamental to combat these crimes at every level.


Please share this guide with any business owners you know, particularly small to medium sized businesses who are at the greatest risk of fraud within company walls.

SHRED STATION

# PHISHING EMAILS

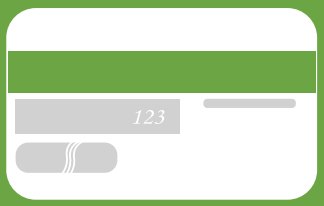
Phishing is a method fraudsters use to trick recipients into performing an action such as clicking on a link or opening an attachment. These links and attachments may contain viruses, and can install malware on the recipient's device. This can then sabotage computer systems and steal data stored on computers such as stored passwords or bank details.

Let your colleagues know about the risks of opening any attachments or clicking on any links that were unexpected. Fraudsters can even imitate your customers or companies in your supply chain, so be sure to check the sender's email address and, if unsure, seek advice from your IT department.

# EMPLOYEE FRAUD

Employee fraud is fraud committed against the company by someone within company walls. This comes in many forms, but one very common form is payment fraud. This is where someone can create a false customer record or invoice for payment, with the payment details being their own bank account or online wallet. It can also come in the form of false expense claims, misrepresentation of skills and qualifications on employee job applications, exploiting company assets (for example, selling customer databases to competitors), and personnel management fraud where staff may be on sick leave but are working elsewhere.

To safeguard against this, you need to rely on your workers. Offer staff a way to anonymously report internal instances.




# INVOICE FRAUD

Fraudsters trick organisations and their suppliers out of huge sums of money each year through invoice fraud. This is where someone impersonating a customer or supplier emails your business saying their invoice details have changed, and all payments should immediately go to the new details provided. They could even impersonate a person from your own company.

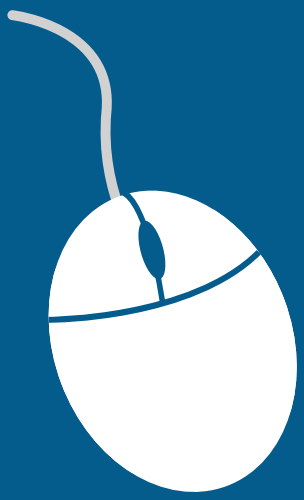
Changing bank and payment details should always be treated with extra caution, and you should double-confirm with the alleged sender via phone or alternative company email address to verify these change in details as a security measure.


## MONEY LAUNDERING

Money laundering is where illegally obtained money goes through the books of a legitimate business to obscure the money's criminal origin.

Be particularly wary if any of your employees - particularly those involved with finances - accept large cash payments often, above what you'd expect and above the amounts accepted by other employees. It's also a good idea to get an anti-money laundering procedure in place.

Money laundering offences are punishable by up to 14 years in prison, a fine, or both. So, it's in your best interest to have measures and training in place to protect yourself and your business.



## IT ATTACKS

IT attacks and cyberattacks are where someone attempts to access, manipulate, delete or steal information from your business through unauthorised online access.

They can expose data through unsecure websites and even your servers if there isn't adequate protection. Hacking, phishing and guessing your employees' passwords can also be used to open up your data to fraudsters.

Cyberattacks are complex. With constant advancements in technology, methods that worked to protect your business from IT attacks and cyberattacks yesterday may not work tomorrow. Your IT department or provider should therefore actively look for any vulnerabilities in your online systems.

## ESPIONAGE

Epsionage is a real threat for any business. The loss or theft of valuable business information and company secrets could have a devastating impact on your company's finances and reputation. Your trade secrets or artefacts could be sold to your competitors, and time and resources could be lost.

Your business should have measures in place to safeguard against the risk of espionage, for example, staff training, securing your premises, and securing your data. You should also limit access to any confidential business information and password protect any documents relating to business innovations. A good way to do this for physical documents is through implementing a clean desk policy and shredding any materials you no longer need.

# PROCUREMENT FRAUD

Procurement fraud is where there is deliberate employee / supplier conspiracy when awarding business contracts, or where a conflict of interest is ignored when issuing contracts.

An example of procurement fraud would be if one of your buyers went against the regular procurement process to award a commercial contract to the business of a friend or family member, or after receiving bribes in the form of cash or gifts from one of the bidding contractors.

You can avoid the risks of procurement fraud by having a clear procurement process in place. This would mean all contract pitches, bids and tenders must meet the exact same criteria to win a contract.

# CEO FRAUD & SOCIAL ENGINEERING

CEO fraud and social engineering is a form of scam where a fraudster will impersonate someone high up in a business to get employees to make urgent payments, purchases, or disclose confidential business information.

This is usually done in the form of an email, asking for an urgent invoice to be paid to a bogus account, or asking an employee to purchase high value online gift cards, and sharing the gift card codes with the "CEO".

Make sure your employees take good care to check email addresses and email signatures when asked to carry out any urgent activity on behalf of any c-suite employees to avoid falling for these costly scams.

These are just a few examples of fraud, and there are many more sophisticated ways that fraudsters operate.

Experian estimates that the annual cost of fraud in the UK is over £190 billion. The majority of this cost is felt by the private sector, with SMEs and large enterprises thought to lose around £144 billion per year. Procurement fraud accounts for a huge portion of this, estimated by Experian to be around £127 billion.

Some of the best ways you can safeguard your business from the risks of fraud is to be particularly wary when it comes to awarding contracts, and receiving any emails or communications pertaining to financial matters that were unexpected.

It's also a good idea to give all staff training around things like password security and common scams to look out for. You should conduct regular accounts audits and offer employees a way to report incidents of suspected fraud within company walls anonymously. If you suspect your employees may be hesitant to report any suspected fraud, incentives could also be offered. After all, your workers could be risking their own working relationships to safeguard your business.

SHRED STATION

# Engaging employees

## REPORTING FRAUD AND PROTECTING WHISTLEBLOWERS

Whistleblowing is where an employee discloses certain types of wrongdoing, such as fraud, in the public's interest.

Whistleblowers may tell their employer directly if they suspect wrongdoing, or they may report their concerns to a solicitor or prescribed person or body. As employers, it is of course best to encourage employees to report concerns internally to resolve any issues, and it's also important to take any concerns seriously. If your employee has been brave enough to speak up about wrongdoing and you dismiss or ignore their concerns, they may be brave enough to go to the media.

An example of a whistleblower could be someone working in a care home who notices that staff members are financially abusing residents. They may report this either to the care home management or to the Care Quality Commission.

Encouraging employees to report fraud and any other unethical behaviour is very important to safeguard your business, your staff and your customers from theft, loss, extortion, or reputational damage. The best way to do this would be to implement a clear reporting procedure that all employees can understand and follow.

As well as relying on your employees to safeguard your business, they also rely on you. If you experience an attack that could compromise your employees' data, such as unauthorised access to HR records, you have a due diligence to let your workers know. This is also the case for any customer or stakeholder data.

## HAVING CLEAR PROCEDURES IN PLACE

As mentioned above, always have a plan in place and a procedure to follow. This includes procedures for employees to report internal wrongdoings, and also the procedures to inform relevant parties about fraudulent activity or data breaches.

## HANDLING DATA RESPONSIBLY

All of your employees and people in your supply chain should be aware of their responsibilities when it comes to the safe handling of data. This includes preventing unauthorised access, only sharing data with approved parties, and safeguarding personal information.

Your business should also have a destruction plan in place for any confidential paper or materials that are no longer needed. A single piece of paper in the wrong bin could be all it takes to cause a data breach - something that could cost your business a substantial sum in fines, not to mention reputational damage. A regular shredding service will save employee time, reduce the risks of data breaches, and help your organisation stay on top of data retention periods.

## RECOGNISING SCAMS AND WHITE COLLAR CRIME

Be proactive in teaching your employees to recognise scams and white collar crime. Without sufficient awareness, something sinister could be missed, and your employees could be unknowingly complicit in crimes.

# Minimising risks

## INTERNAL FRAUD

With fraud cases consistently rising, noticing the signs of internal fraud has never been more important. We've highlighted some of the most common warning signs below.


- Unusually close, secretive relationships with certain suppliers or customers.
- Financial difficulties or change in circumstances e.g. divorce.
- Living beyond their means with no apparent explanation.
- Unwillingness to share duties or displaying control issues.
- Large volumes of cash-only transactions or large volumes of refunds to certain customers.
- Opportunity to commit the crimes - especially those working in finance or accounts.
- Regularly working later than everyone else.
- Unwillingness to take long holidays or time off.
- Frequently aggressive when challenged or showing excessive stress for their pressures.

Early detection and prevention of fraud crimes is essential for any business. The longer these crimes go unnoticed, the more damage will be done. This is true for financial damage, reputational damage, damage to your business relationships and, of course, any potential legal ramifications. These are some of the best ways to minimise risks.

**REPORTING PROCEDURE**
Implement a clear reporting procedure for staff to follow to report suspected incidents of fraud.

**STAFF TRAINING**
Give all staff training on data security, financial security, and how to recognise fraudulent activity.

**MANAGE RISKS**
Implement systems, such as AI or staff policies, to detect the early warning signs of potential fraud.

**REGULAR MONITORING**
Conduct regular financial audits, both internally and using external auditors, to monitor any anomalies.

**RESPONSE PLAN**
Have a response plan in place before any incidents of fraud occur to minimise potential damage.

SHRED STATION

# Minimising risks

## EXTERNAL FRAUD

While internal fraud is detectable through internal controls, audits, and caution from staff, customers, and suppliers - usually after the fact - external fraud requires more proactive ways of prevention. This includes actively searching for potential areas of vulnerability, having measures in place to manage data, and much more.

### PERFORM PRACTICE EXERCISES

Practice exercises are a great way to teach your teams how to respond to cyberattacks.

The National Cyber Security Centre has a very useful online 'Exercise in a Box' tool that can show how resilient your organisation is to cyberattacks, and give your IT team a way to test their responses in a safe, no-risk environment.

### PROVIDE STAFF TRAINING

Your team is your best asset, and by training your staff on fraud awareness you could prevent what may have been a successful external fraud attempt. There are many training programmes available online for businesses to use to train staff about fraud, as well as free resources. Practice exercises are also a great training method against potential risks like phishing or CEO fraud.

### IMPLEMENT ACCESS CONTROLS

To stop unauthorised access to any data, internally or externally, you should have strict access controls in place. This goes for physical data and digital data.

Physically, you should install secure entry facilities such as key-code entry, visitor sign-in machines, and lockable doors and cupboards for any areas where confidential materials are kept.

Digitally, your confidential information should be kept away from shared drives, have password protection on documents if neccessary, and you should encrypt all devices. Password protections should also be in place, and any digital accounts such as CRM systems should be limited in access and have multi-factor authentication enabled.

### INVEST IN CYBERSECURITY

Unforeseen events such as malicious fraud attempts and accidential vulnerabilities can be safeguarded against by investing in enhanced cybersecurity.

Your internal or external cybersecurity experts should conduct a cyber resilience plan to evaluate your organisation's cyber hygiene. From this plan they can implement hygiene measures such as anti-malware and firewalls, VPNs, software patches and updates, device security, encryption, and more.

### ACTIVELY LOOK FOR VULNERABILITIES

It is no longer enough to implement cybersecurity measures without actively looking for vulnerabilities. As software and technology is regularly updated, what may have worked to protect your business one day may not work the next. Fraudsters and hackers are always developing their skills and methods to gain unauthorised access to data, so your cybersecurity team should continuously be on the lookout for any vulnerabilities or potential areas of risk.

### IMPLEMENT REPORTING PROCEDURES

If a successful fraud attempt exposes any personal information, and this exposure could affect people's rights and freedoms, you are legally obliged to inform the Information Commissioner's office within 72 hours. If your business relies on investors, you also need to inform investors of any incidents. To not disclose these incidents is a form of fraud against the investor in itself.

To make reporting, internally and externally, as simple as possible, you should implement a reporting process that all staff can access immediately.

### DESTROY MATERIALS SECURELY

Any confidential materials or materials that could pose a risk to your organisation in the wrong hands should be securely destroyed by a specialist service provider. This goes for paperwork, unwanted hard drives, digital media storage devices, old uniforms, and anything else that could contain confidential or personal information.

SHRED STATION

# Online account security

## CYBER HYGIENE & ONLINE DATA SECURITY

Cyber hygiene, as we touched on in the previous page, is a vital part of online account security and cybersecurity. So, without getting too technical, how can your business implement cyber hygiene measures?

### HAVE AN UP-TO-DATE INVENTORY

Keep an up-to-date record of who has company-issued devices, and who has access to your internal systems. This will allow you to limit access once employees have left the business.

### TRACK ACTIVITIES WITH ENHANCED LOGGING

Logging who has accessed what information - and why - is vital. If your business does have a data breach, you need to be able to trace where it originated and what information was compromised. Logging tools can help your IT department see the data trail for every action on your networks, systems and shared drives.

### ENSURE SECURE ACCESS

Limiting access to confidential information isn't just vital for data security, it's also a requirement under UK GDPR. No unauthorised person, either internally or externally, should be able to access any confidential or personal data unless they absolutely need to. This goes for both physical and digital data.

### INVEST IN DIGITAL CERTIFICATES

If your business has a website, you need an SSL certificate. An SSL is a small file that confirms your website's authenticity and enables encrypted connection for your site users. When you have an SSL, your website users will see the padlock icon before your URL and your https status. This lets your site users know their session is secure and your website can be trusted. It also means any data entered on your web forms or payments made on your site are secure.

### IMPLEMENT A PASSWORD POLICY

By having a clear set of rules about password strength and multi-factor authentication, your employees can protect their online accounts from hacking. You can also increase password controls by enabling password expiration on certain logins. If passwords are unknowingly breached, this will shorten the window of opportunity for the attacker to act.

### REGULARLY BACK UP DATA

There are few things more stressful for businesses than being victim to fraud or hacking, and these issues can be made significantly worse if your business data is not backed up. By backing up your data, you're protecting yourself from losing hours of work and vital business information.

### INSTALL SOFTWARE UPDATES AS SOON AS AVAILABLE

Software and computer updates might seem like a bit of an annoyance for your employees who need to stop what they are doing to install updates, but updating software as soon as possible is very important. Updates to software may fix known bugs, issues, or even patch vulnerabilities. If your employees aren't updating their software, their systems may be at risk.

### TEST, TEST, AND TEST AGAIN

As technology evolves, complacency could mean your IT team misses a potential vulnerability in your online systems. Continuous testing and monitoring will help your teams stay on top of any potential risks of fraud or hacking.



SHRED STATION

# Data breaches & how to report them

## WHAT IS A DATA BREACH?

The Information Commissioner's Office defines a personal data breach as "a security incident that has affected the confidentiality, integrity or availability of personal data". Your business should have measures in place, such as those mentioned throughout this document, to safeguard against such incidents. You should also have a reporting procedure in place to identify and report incidents internally and to the Information Commissioner's Office and affected parties if necessary.

There are also data breaches that may not contain personal data, but could hurt a business financially. For example, the loss of product prototypes, financial data, or company secrets. These do not necessarily have to be reported to the Information Commissioner's Office, but that doesn't mean to say you shouldn't have procedures in place internally to report these issues to relevant employees, stakeholders, your suppliers, investors, or clients.

## USEFUL RESOURCES

The Information Commissioner's Office is the UK's independent authority that exists to uphold information rights in the public's interest. The Information Commissioner's Office has lots of free, useful resources online to help your business with safeguarding confidential information in line with the UK General Data Protection Regulations and everything else you need to know to protect your information from being breached.

You can visit their website at: **https://ico.org.uk/**

## REPORTING A DATA BREACH TO THE INFORMATION COMMISSIONER'S OFFICE

There are certain incidents that require organisations to report data breaches to the Information Commissioner's Office. For most businesses, this pertains to the unlawful or accidental destruction, loss, alteration, unauthorised access of, or unauthorised disclosure of personal data. If such a data breach occurs, you need to consider the likelihood and severity of the risk to people's rights and freedoms. If the breach is likely to affect people's rights and freedoms, **you are legally required** to notify the Information Commissioner's Office within 72 hours of discovery.

For more information on how to report a data breach at your organisation, visit the Information Commissioner's Office's website:
**https://ico.org.uk/for-organisations/report-a-breach/**

# Handling data securely

In addition to the fraud techniques already mentioned, physical information is also a huge area of risk when it comes to commercial fraud and espionage. A single piece of paper in the wrong hands could constitute a data breach and could expose enough business information to cause reputational damage, loss of assets, loss of income, and fines. The best way to ensure your physical materials aren't exposing your organisation to the risk of a data breach is to destroy anything you no longer need. This goes for invoices, employee notebooks, post-it notes, archived paperwork, old HR records, uniforms, hard drives, and any other material that could be used to sabotage your business.

Here are some quick tips on how to avoid your confidential materials getting into the wrong hands.

- **Implement a 'Shred Everything' policy and install confidential waste bins.**

Bin raiding is a common practice fraudsters use whereby they take documents out of bins, using these documents to commit fraud. To avoid employees making the wrong call when it comes to what data to keep and what to destroy, implement a 'Shred Everything' policy for all documents and data storage devices that are no longer needed. Install lockable confidential waste bins or cabinets at every site so this process is easy for your employees, and have these bins' contents collected regularly for secure destruction.

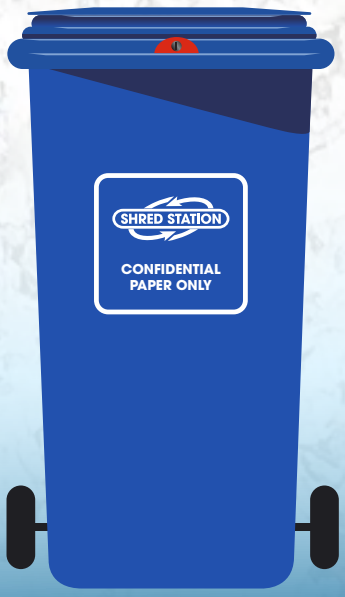
- **Use CCTV, premise access controls, and keep confidential materials locked away and out of sight from any windows or doors.**

Criminals often stake out properties before break-ins, considering things like when offices or workplaces will be empty and what valuables they can get their hands on inside. You can protect your business from break-ins and data theft by installing CCTV, alarmed doors, entrance security, and by making sure all documents and devices are locked away, both when not in use and at the end of the working day.

- **Ensure employees are aware of how data should be safeguarded.**

Make sure your employees are aware of the common fraud methods used to target businesses. If they receive any unusual requests regarding urgent invoices, or for copies of customer files, they should be aware of the procedures to follow and the risks involved.

Staff who handle personal information such as HR or hiring managers should be very cautious when they handle applicant and employee data. CVs, for instance, should never be left unattended on desks or where they may be visible to other employees.



# Destroying data securely

When you no longer need your confidential materials, you should destroy them to avoid them falling into the wrong hands. Using a fully-accredited shredding service is the best way to do this and is much more secure than using an office shredder. Office shredders require ongoing maintenance and often shred documents into long strips, which are easy to reassemble. With office shredding, your fragments may also just end up outside in an unlocked bin, ready for the taking.

When you use a shredding service, your material will be destroyed by industrial shredders operated by security-vetted personnel. These machines tear your items into small pieces. Your fragments will also be mixed with hundreds of thousands of others, never accessible to the public.

At Shred Station, we want our customers to feel confident about data destruction. We give our customers this confidence by having high security measures in place every step of the way. We also do our best to minimise our environmental impacts, cause minimal interruption to our customers, provide industry-leading customer service, and continuously innovate. All of this combined means we offer a service to suit all businesses. You'll even receive a Waste Transfer Note and Certificate of Destruction for your compliance records after every service.


1

## Schedule Collection

Lockable bins or bags are supplied for regular collections, or alternatively we offer a one-off collection of bagged, boxed or palletised material.

## Our Journey Begins

You'll receive an email containing a live service tracking link. You can track our driver's route position throughout the day. You'll also receive a second email when you are the next job on our driver's route.

2


## Security Vetted Staff

Our uniformed and BS7858 security-vetted staff will transfer your documents and material into a secure vehicle.

3



4

## Off-site Shredding

Secure vehicle is sealed for transportation and material is shredded on arrival at our secure depot.

**OR**

## On-Site Shredding

Once behind secure doors, our operatives place the data directly into the shredder located on board.


5

## Certificate of Destruction & WTN

A certificate of destruction and **waste transfer note** are issued, confirming the safe destruction of your data in compliance with European standards.


## Recycling

Shredded paper is baled and sent to UK mills for recycling. Other material is recycled where possible and non-recycleables are sent to Energy from Waste. Nothing we shred goes to landfill.

6