Be Vigilant of Fraud

Scammers can often take advantage of busy schedules and online shopping trends for businesses.

Protect yourself and your business by staying alert and following these essential tips:

Be Wary of Unexpected Messages

- Emails, texts, or calls claiming to be from banks, delivery companies, or government agencies may be fake.
- Never click on suspicious links or download attachments from unknown sources.
- If in doubt, contact the company directly using official details.

Watch Out for Fake Shopping Deals

- Scammers create fake websites offering huge discounts.
- Check for secure payment options (look for "https://" and a padlock symbol).
- Avoid deals that seem too good to be true—they usually are.

Protect Your Personal Information

- Never share bank details, passwords, or PINs via email or phone.
- Use strong, unique passwords and enable two-factor authentication where possible.

Stay Alert to Charity Scams

- Winter is a time for giving, but scammers exploit generosity.
- Donate only through official charity websites or trusted platforms.
- Verify charities on the Charity Commission register before donating.

Beware of Energy Bill and Cost-of-Living Scams

- Fraudsters may offer fake discounts or rebates.

- Always check with your energy provider directly before making payments.

Fake Investment Opportunities

- Promises of quick returns on cryptocurrency or stocks.
- Pressure to invest immediately.
- Always research and seek advice from a regulated financial advisor.

Romance & Friendship Scams

- Increased loneliness during winter can lead to exploitation.
- Scammers build trust online before requesting money.
- Never send money to someone you've only met online.

Cybersecurity Threats

- Increased phishing emails disguised as holiday greetings or invoices.
- Malware hidden in attachments or links.
- Always keep systems updated and train staff on phishing awareness.

Invoice & Supplier Fraud

- Scammers send fake invoices or impersonate suppliers requesting urgent payments.
- Often timed during busy periods when staff are distracted.
- Always confirm all payment requests through official channels before processing.

Fake Recruitment Scams

- Scammers pose as job seekers or agencies, sending malware-laden CVs.
- Always use secure recruitment platforms and scan attachments before opening.

Stay vigilant, protect your personal and business information, and report suspicious activity to Action Fraud: https://www.actionfraud.police.uk/

Refund Scams: Protect Your Business

One to watch out for are refund scams, which are on the rise targeting businesses of all sizes. Scammers often pose as genuine customers and exploit refund processes to steal money. Here's what you need to know:

What is a Refund Scam?

A refund scam occurs when fraudsters trick businesses into issuing refunds for goods or services they never purchased or for transactions that never occurred. Common tactics include:

- Fake receipts or invoices claiming a purchase was made.
- Phishing emails pretending to be from payment providers or banks.
- Chargeback fraud, where a scammer disputes a legitimate transaction after receiving goods.

How to Spot a Refund Scam

- Requests for refunds without proof of purchase or with suspicious documentation.
- Pressure to refund quickly, often citing urgency or emotional reasons.
- Refund requests to different accounts than the original payment method.
- Poor grammar or unusual email addresses in correspondence.

How to Protect Your Business

- Verify all refund requests against your transaction records.
- Only issue refunds to the original payment method.
- Train staff to recognize red flags and follow strict refund policies.
- Use secure payment systems and enable fraud detection tools.
- Report suspicious activity to Action Fraud and your payment provider.

Stay vigilant, protect your personal and business information, and report suspicious activity to Action Fraud: https://www.actionfraud.police.uk/

Credit Card Machine Refund Scam Explained

A refund scam occurs when a criminal manipulates a card terminal to process unauthorized refunds to their own card or account. This often happens in retail or hospitality settings where staff have access to the machine.

How It Works:

- The scammer initiates a refund without a corresponding sale.
- They enter their own card details or insert their card into the machine.
- The refund is processed, and the funds are transferred from the business account to the scammer's account.
- In some cases, scammers may trick staff into processing the refund by claiming they were overcharged or returning goods they never purchased.

Risks:

- Businesses lose money directly from their merchant account.
- Chargebacks and disputes can lead to additional fees.
- Repeated incidents can damage reputation and lead to compliance issues.

Warning Signs:

- Refunds processed without matching sales records.
- Staff overriding security checks or skipping manager approval.
- Frequent refunds to the same card or account.

Prevention Tips:

- Require manager authorization for all refunds.
- Enable refund limits and audit logs on terminals.
- Train staff to verify original transactions before issuing refunds.
- Monitor daily reports for unusual refund activity.

Stay vigilant, protect your personal and business information, and report suspicious activity to Action Fraud: https://www.actionfraud.police.uk/