Visa Fraud and Security Toolkit

Stand Up to Fraud

A practical guide for small to medium sized businesses

VISA

Safeguarding your small business against potential risks and threats

Running a small to medium-sized business (SMB) can be a rewarding if sometimes challenging experience. Business owners need to manage a range of issues, from creating a great customer experience and managing finances, to staying competitive and increasingly, addressing the rising threat of fraud. At Visa, we believe in providing SMBs with the tools and confidence they need to thrive in the digital economy. Our priority is keeping money safe from fraud to provide peace of mind for businesses and their customers. We are now going one step further with this toolkit, which is designed to help you understand the different types of fraud that threaten SMBs, better assess the risks to your business, and take practical steps to keep your business, and your customers, secure. By helping you make informed decisions to reduce the risk of fraud, we want to help you get back to what you do best: growing your business.

We invite you to dive in, explore the resources, and take proactive steps to protect your business from potential threats.

41%

More than two fifths of SMBs in the UK have fallen prey to fraud and scams[1]

£4k

On average, SMBs in the UK lose £4k each year to fraud and scams[1]

Identifying, preventing and acting on the most common types of scams and fraud

As part of our ongoing commitment to preventing fraud, we have identified the most common types of scams and fraud that small to medium-sized businesses experience. Learn how to protect your company from falling victim to them:

Contents

Phishing scams

Phishing scams trick people into giving away sensitive information like passwords, credit card details, or financial data by pretending to be a trusted source, such as a real bank or phone network. Scammers often use fake emails or websites to deceive victims. They may also use text messages (Smishing) or phone calls (Vishing) to achieve the same goal. These scams often create a sense of urgency to make people act quickly. Once successful, phishing can lead to identity theft, financial loss, or access to personal accounts.

24%

Almost a quarter (24%) of SMB fraud cases reported were phishing scams[1]

75%

Almost three quarters (75%) of SMBs agree that improving digital capabilities are the most effective methods for preventing fraud[1]

Illustrative example

An example of a phishing scam

Jenny runs a furniture business in Birmingham. One day, her assistant, Sarah, receives an email that appears to be from the company's bank, requesting urgent account verification to avoid suspension. The email looks convincing, so Sarah clicks the link and enters the business's banking login details. Unbeknownst to her, the website is a fake, set up by fraudsters to steal the company's credentials. By the next morning, Jenny discovers that the company's bank accounts have been emptied, causing a significant cashflow issue.

What action is recommended?

1. Contact the bank immediately to report the fraud and request that the accounts be frozen and investigated.

2. Disconnect the computer used to enter the details to stop any further fraudulent activity.

3. Report the incident to Action Fraud and the Information Commissioner's Office (ICO) to investigate the phishing attack and potential data breach.

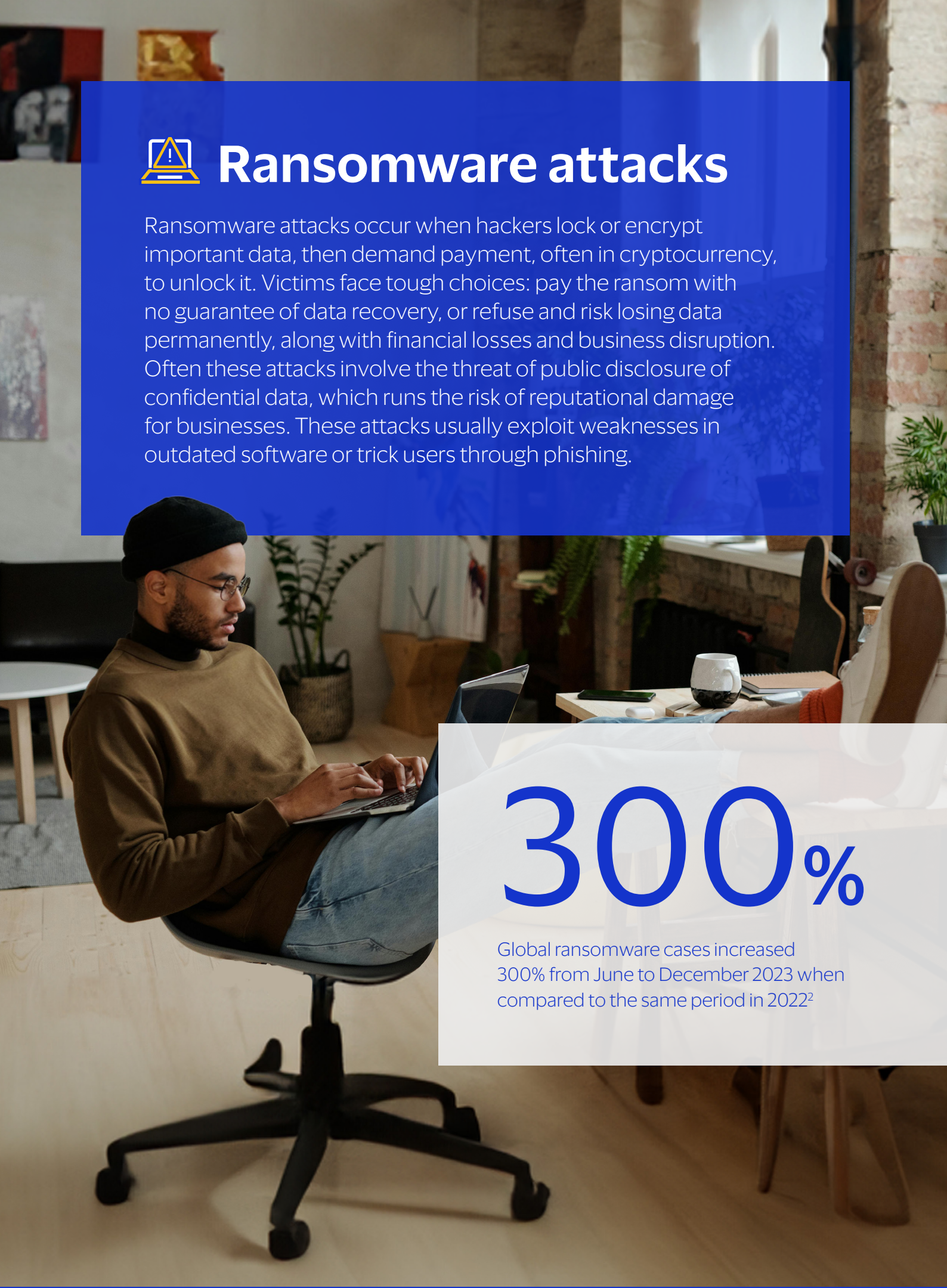
4. Hire an IT security specialist to scan the system for malware and boost cybersecurity to prevent future attacks.

5. Train up on how to recognise phishing emails and suspicious links to avoid similar incidents in the future.

Safeguarding tips

To safeguard against phishing, smishing and vishing scams, we recommend using the following tactics:

- Train yourself and employees to recognise phishing messages, suspicious links, and attachments to reduce the risk of scams.
- Use multi-factor authentication (MFA) to add an extra layer of security beyond just passwords.
- Ensure you and your staff use strong, unique passwords and update them regularly with password management tools.
- Regularly update all software to fix vulnerabilities that hackers might exploit.
- Install email filters to block potential phishing emails from reaching you and your team's inboxes.



Ransomware attacks

Ransomware attacks occur when hackers lock or encrypt important data, then demand payment, often in cryptocurrency, to unlock it. Victims face tough choices: pay the ransom with no guarantee of data recovery, or refuse and risk losing data permanently, along with financial losses and business disruption. Often these attacks involve the threat of public disclosure of confidential data, which runs the risk of reputational damage for businesses. These attacks usually exploit weaknesses in outdated software or trick users through phishing.

300%

Global ransomware cases increased 300% from June to December 2023 when compared to the same period in 2022[2]

Illustrative example

An example of a ransomware attack

Shayma runs a successful dentistry clinic in Bristol. Her clinic manager Mika receives an email claiming to be from the industry association for dentistry, stating that the clinic's details need to be updated, with a link in the email. Mika clicks on the link and doesn't realise that he has inadvertently downloaded malicious software that allows the attackers to access the clinic's patient database. The attackers then lock the clinic work stations, demanding payment in cryptocurrency, or they will sell on all the patient data. The attackers also state that Mika and the clinic will be liable to be sued by their patients for not protecting their private data. Mika is given a deadline of 48 hours.

What action is recommended?

1. Disconnect the clinic's workstations from the internet to prevent further access by attackers.

2. Report the incident to the appropriate authorities, such as the Information Commissioner's Office (ICO) in the UK, and provide details of the ransomware attack and potential data breach.

3. Contact a professional IT security firm to assess the extent of the breach, remove the malicious software, and restore access to the patient database.

4. Inform patients about the breach and reassure them that the clinic is taking steps to address the situation and protect their data.

5. Refrain from paying the ransom as it encourages further attacks and does not guarantee the safe return of data. Instead, focus on restoring systems and improving cybersecurity measures.

Safeguarding tips

You can protect your business from ransomware attacks with a multi-layered cybersecurity strategy:

- Regularly back up data offline or in the cloud to recover quickly without paying a ransom.
- Keep all software updated to close any security gaps ransomware can exploit.
- Train yourself and employees to avoid phishing attacks and use safe online practices to prevent malware.
- Use strong antivirus software and tools to detect and stop ransomware early.
- Create a plan to quickly respond and recover if a ransomware attack happens.

Billing fraud and false invoices

Fraudsters may pose as legitimate suppliers or send fake invoices, tricking businesses into paying for goods or services they never received. Insiders could also alter billing systems or inflate invoices to steal money. These scams cause financial losses and can harm vendor relationships. Without proper checks, billing fraud can go unnoticed, resulting in product or service shortages and threatening your business's financial stability.

26%

Billing fraud and false invoicing is the most common type of fraud for small to medium-sized businesses (26%)[1]

Illustrative example

An example of billing fraud and false invoicing

Tariq runs a small manufacturing company in Sheffield. He receives an email which appears to be from their regular supplier, requesting payment for an urgent invoice. The email claims the supplier has changed their bank details and provides new account information. Trusting the request, Tariq updates the payment details and transfers £10,000. Later, the supplier contacts Tariq, confused about the missing payment. The scammer, posing as the supplier, disappears with the funds.

What action is recommended?

1. Contact the bank immediately to see if they can freeze the transaction.

2. Report the incident to authorities, such as Action Fraud.

3. Inform the legitimate supplier about the fraudulent email and payment.

4. Review and enhance the company's cybersecurity measures.

5. Consider seeking legal advice for potential recovery options.

Safeguarding tips

Safeguarding against billing fraud and false invoices requires a mix of preventive steps and careful monitoring:

- Vet new vendors carefully and regularly review existing ones to ensure they are legitimate.
- Implement strict approval processes and require multiple levels of authorisation.
- Train yourself and staff to understand billing fraud and always verify invoices before processing payments.
- Use accounting software to detect issues like duplicate invoices or unusual billing patterns.
- Perform regular audits to spot discrepancies or suspicious activity in financial records.

Authorised Push Payment (APP) fraud

Authorised Push Payment (APP) fraud occurs when fraudsters trick victims into authorising transactions. Often fraudsters will impersonate an individual or organisation, such as a bank or a parcel delivery service and trick the victim into transferring money from their account into an account held by the fraudster. Typically the fraudster will contact the victim via telephone, text message or email to trick them into handing over their personal details or passwords. As of 2024, new APP fraud reimbursement protections mean that victims can make a claim to get their money back.

£213.7m

Authorised Push Payment (APP) fraud losses totalled £213.7 million in the UK in the first half of 2024[3]

Illustrative example

An example of Authorised Push Payment fraud

Salima, the owner of a small architectural firm in the UK, receives an urgent call from someone claiming to be a tax official from HMRC. The caller explains that Salima owes a significant tax amount and must make an immediate payment to avoid penalties. Feeling under pressure, Salima is instructed to transfer the funds via the Faster Payments System to the provided bank details. The caller uses pressure tactics, stressing the urgency and legal repercussions if the payment isn't made immediately. Shortly after, Salima realises the payment might have been a scam.

What action is recommended?

1. Immediately contact the bank to try to stop the transaction and request a recall or reimbursement claim if the payment was fraudulent.

2. Report the fraud to Action Fraud and notify HMRC about the scam to ensure proper authorities are aware.

3. Verify any communication claiming to be from government agencies by contacting them directly through official channels.

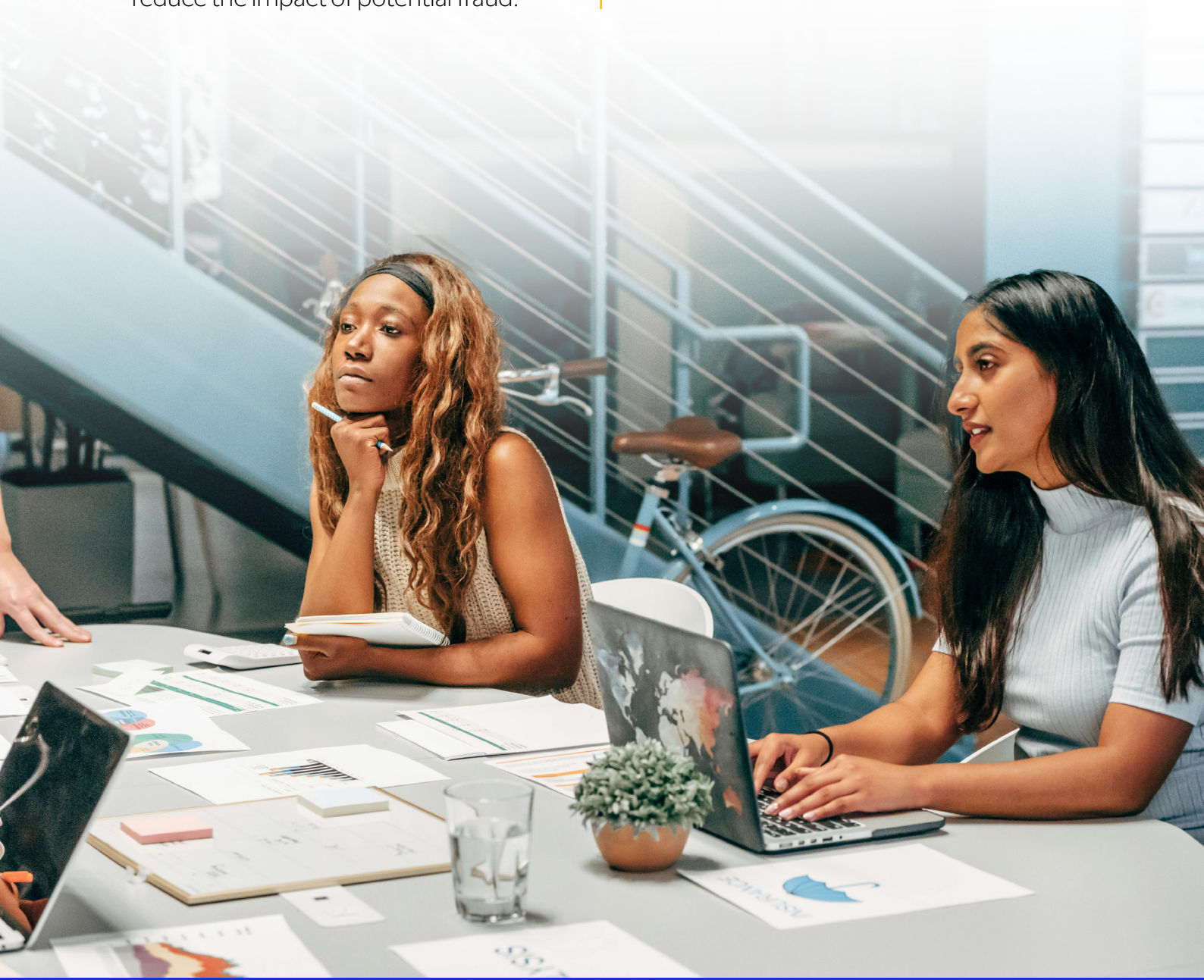
4. Review the business's payment processes and implement safeguards to verify unexpected or urgent payment requests.

5. Train up on how to recognise suspicious payment requests and avoid authorising any transactions without proper verification.

Safeguarding tips

The following tips can help businesses safeguard against Authorised Push Payment fraud:

- Always verify any unexpected or urgent payment requests by contacting the sender directly through official and trusted channels.
- Regularly monitor your bank accounts for any unusual or suspicious activity that could indicate fraudulent transactions.
- Set daily limits on the amount and frequency of instant transfers to reduce the impact of potential fraud.
- Familiarise yourself with the new APP fraud reimbursement claim process.
- Train yourself and staff to recognise phishing and social engineering tactics commonly used by fraudsters to request unauthorised payments.



Remote purchase / card-not-present fraud

Remote purchase fraud occurs when a fraudster steals financial information through phishing, malware or data breaches, enabling them to make fraudulent purchases. This is referred to as card-not-present (CNP) fraud when stolen card details are used for online or phone purchases without the card being physically present. This type of fraud can lead to significant financial losses for businesses through chargebacks, as they are often held responsible for recovering the money lost by the customer.

26%

The number of card-not-present (CNP) fraud cases increased by 26% in the UK in the first half of 2024[3]

Illustrative example

An example of remote purchase / card-not-present fraud

Miriam, the owner of an e-commerce store, notices unusual activity on her website. Multiple back-to-back orders are placed from the same name and email but using different credit cards. While Miriam's average order consists of three items, one order includes 54 items, and the shipping addresses don't match the billing information. This suggests potential card-not-present (CNP) fraud. Miriam isn't sure if she should process the order, as if it's fraudulent she will have to refund the victim and lose out on the value of the sale.

What action is recommended?

1. Examine the suspicious orders for signs of fraud, such as mismatched billing and shipping addresses, unusually large orders, or different credit cards.

2. Contact the customers to verify the legitimacy of these transactions and confirm if they authorised the purchases.

3. Implement enhanced security measures by adding verification steps like 3D Secure, CAPTCHA, or CVV requirements for large or suspicious transactions.

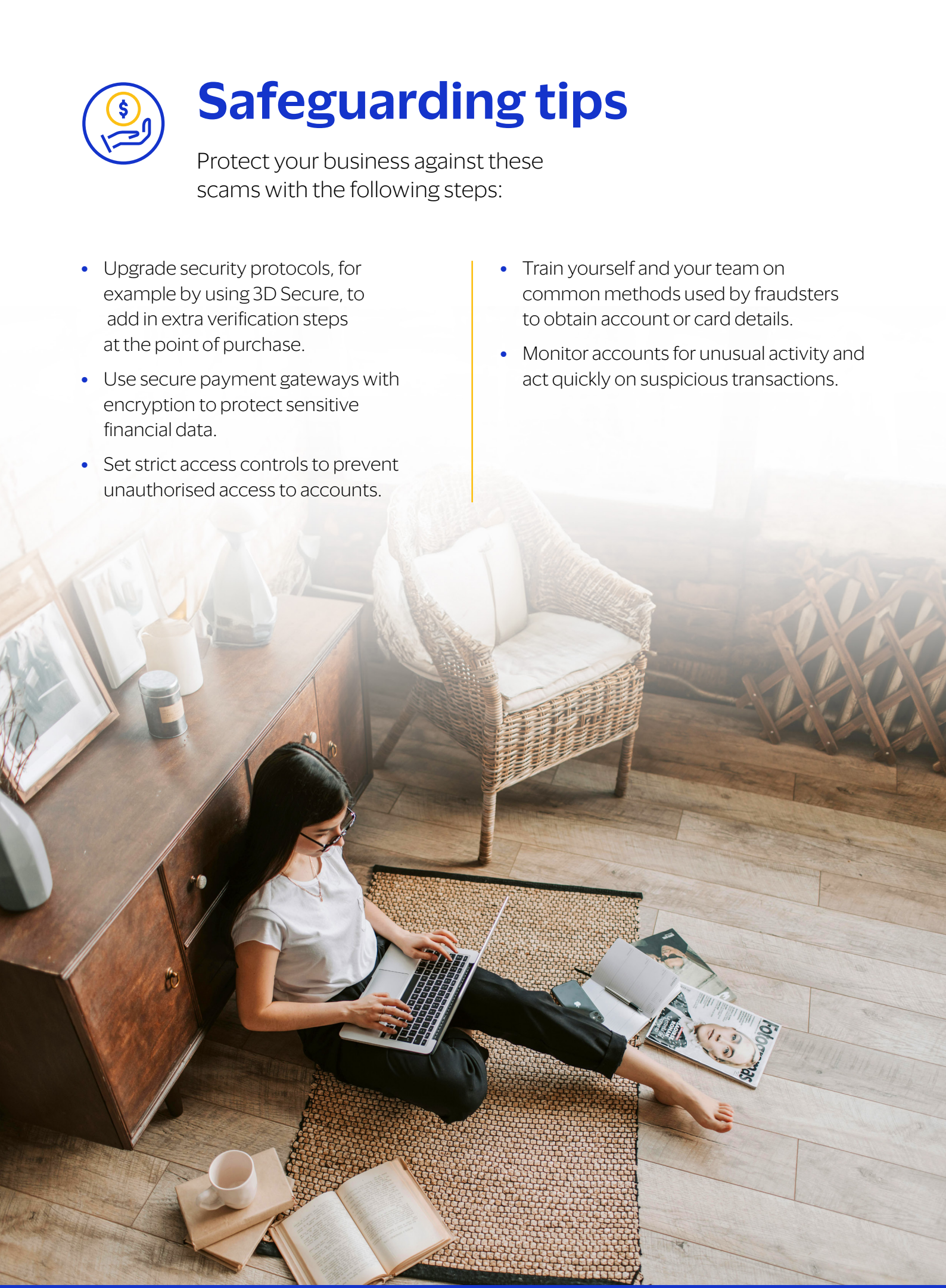
4. Monitor the website closely for further signs of CNP fraud, flagging unusual activity, and acting swiftly to prevent further loss.

5. Report the fraud to Action Fraud or relevant authorities in the UK to investigate and take legal action if necessary.

Safeguarding tips

Protect your business against these scams with the following steps:

- Upgrade security protocols, for example by using 3D Secure, to add in extra verification steps at the point of purchase.
- Use secure payment gateways with encryption to protect sensitive financial data.
- Set strict access controls to prevent unauthorised access to accounts.
- Train yourself and your team on common methods used by fraudsters to obtain account or card details.
- Monitor accounts for unusual activity and act quickly on suspicious transactions.



Fraudulent chargebacks

Fraudulent chargebacks happen when fraudulent customers falsely dispute transactions, claiming they were unauthorised. This causes funds to be returned to the customer, leading to financial losses and reputational damage for the business. Fraudsters often use stolen card details, identity theft, or make false claims (friendly fraud) to trigger chargebacks. Businesses face the challenge of proving legitimate transactions, plus risk penalties, higher fees, or even losing their merchant accounts if chargebacks become excessive.

75%

First party misuse accounts for up to 75% of all chargebacks[4]

Illustrative example

An example of a fraudulent chargeback

John, who runs a small online retailer, sells an electric heater to a customer, who later files a chargeback claim, alleging non-receipt of the item. John provides proof of delivery, but the customer persists, claiming they never received it. The bank initiates a chargeback, refunding the customer. John is left without payment, facing financial loss and product depletion.

What action is recommended?

John should take the following actions:

1. Compile all relevant documentation, including proof of delivery and communication with the customer.

2. Provide the bank with evidence to dispute the chargeback and request a review of the case.

3. Attempt to resolve the issue directly with the customer to clarify any misunderstandings or concerns.

4. Assess company policies regarding chargebacks and consider updating them if necessary.

5. Implement measures such as signature confirmation or insurance for high-value items to mitigate future chargeback risks.

Safeguarding tips

Safeguard against fraudulent chargebacks with preventive measures and proactive strategies:

- Use fraud detection tools to monitor transactions in real time.
- Implement strong authentication and address verification for online purchases.
- Keep detailed transaction records and respond quickly to disputes.
- Train yourself and staff to recognise fraud signs and handle transactions securely.
- Set clear refund and return policies to manage customer expectations and avoid disputes.

Enumeration and card testing attacks

Enumeration fraud and card testing attacks happen when criminals try to confirm stolen card details through payment systems. In enumeration fraud, attackers use automated programmes to guess card information like the CVV or expiration date. Card testing involves making small purchases or donations to check if the stolen card details are still valid. Both methods are used to find active cards for larger fraudulent transactions. These attacks can lead to financial losses and more chargebacks for businesses.

40%

Enumeration attacks increased 40% globally during the period between January - June 2023[5]

Illustrative example

An example of an enumeration and card testing attack

A small charitable organisation began noticing unusual activity on their donation platform. Over a few days, they saw a significant increase in failed transactions and small donation amounts under £5. After investigating, the Finance Director Marina realised they were victims of a card testing attack, where fraudsters use their donation site to validate stolen credit card details. This activity not only jeopardised their financial security but also threatened their reputation and donor trust.

What steps should be taken?

1. Contact the payment processor to report fraudulent activity and get help with additional security measures.

2. Engage with an IT security provider for a thorough assessment and security recommendations.

3. Consult the web developer to implement CAPTCHA, device fingerprinting, and secure coding practices.

4. Notify the banking institution to monitor for suspicious activity and collaborate on fraud prevention strategies.

5. Consult with legal counsel to understand the implications of the attack and ensure regulatory compliance.

Safeguarding tips

Businesses can implement several strategies to mitigate against enumeration fraud and card testing attacks:

- Add anti-automation tools like CAPTCHA to checkout pages to block bots.
- Use firewalls and detection tools to identify botnets and prevent attacks.
- Limit the number of transactions allowed within a short time to stop rapid attempts.
- Track unusual traffic spikes or patterns in form entries to catch threats early.
- Set minimum transaction amounts to discourage card testing with low-value purchases.

Skimming fraud

Skimming fraud occurs when criminals use a device, called a skimmer, to steal credit or debit card information. These devices are secretly attached to card readers at places like ATMs, petrol pumps, or self-service checkouts. The skimmer captures the magnetic stripe data from the card, which criminals can then use to create counterfeit cards or make unauthorised purchases. Fraudsters may also use hidden cameras or overlays to capture PIN numbers, allowing them to make withdrawals or fraudulent transactions with the stolen information. Skimming can lead to significant financial losses for businesses and customers.

174%

Skimming attacks increased by 174% globally between June and November 2022 compared to the previous six months, with a growing impact in Europe[6]

Illustrative example

An example of skimming fraud

A small, independent coffee shop in London, started receiving complaints from customers about unauthorised transactions on their bank accounts after using the café's card payment system. Upon investigation, owner Mahmoud discovered that a skimming device had been secretly attached to the POS terminal, stealing customers' card data. The fraud not only put customer trust at risk but also posed serious financial and reputational threats to the business.

What action is recommended?

1. Immediately disconnect the compromised POS terminal and replace it with a secure system, such as one with EMV chip protection.

2. Report the fraud to the bank and payment processor to stop further fraudulent transactions and seek support with chargeback issues.

3. Engage a security expert to inspect the premises for other devices and recommend stronger security measures.

4. Notify affected customers promptly, offering guidance on monitoring their accounts and contacting their banks to mitigate damage.

5. Report the incident to the police and Action Fraud to support a broader investigation and prevent future attacks.

Safeguarding tips

Businesses can implement several strategies to mitigate against skimming fraud:

- Regularly inspect payment terminals for signs of tampering, such as loose card readers, unfamiliar attachments, or damaged parts.
- Use EMV chip-enabled terminals and contactless payment methods, which are more secure than magnetic stripe cards against skimming.
- Train yourself and staff to recognise signs of skimming devices and report any suspicious activity around card readers immediately.
- Install tamper-evident seals on POS terminals, and monitor them regularly to detect any signs of unauthorised access.
- Encourage customers to cover the keypad when entering their PIN and to use digital wallets for added security.

Tackling fraud:

How ready is your business?

Businesses can stay one step ahead of fraudsters by taking a proactive approach. It's important to teach yourself, as well as your employees and customers how to spot the risks and stay safe.

Here are eight key strategies to fight fraud:

1. Conduct fraud training:
Train yourself and employees to identify phishing emails and suspicious activity to minimise the risk of scams.

2. Implement Multi-factor Authentication (MFA):
Implement MFA for all systems to add an extra layer of security and reduce unauthorised access.

3. Enforce strong password policies:
Ensure yourself and your staff use unique, complex passwords and update them regularly with password management tools.

4. Perform regular software updates:
Keep all software, including antivirus programmes, updated to patch vulnerabilities and prevent attacks like ransomware.

5. Verify payment requests
Always confirm any unexpected payment requests by contacting the requester directly through official channels.

6. Monitor transactions:
Regularly monitor accounts for unusual or suspicious activity, acting quickly to prevent fraudulent payments.

7. Secure payment systems:
Use third-party fraud services to provide additional protection and real-time transaction monitoring.

8. Develop a response plan:
Create a response plan so you're clear on the steps to take to protect your business and your customers in the event of a scam.

Useful resources

Practical Business Skills: Security and fraud
Learn what steps you can take to prevent fraud and data theft to protect your business and your customers on the Practical Business Skills website.

Practical Business Skills website

Small Business Guide: Cyber Security
Get affordable, practical advice for businesses to improve cyber security.

National Cyber Security Centre website

Stop! Think Fraud
Giving you the knowledge and tools you need to stay ahead of scams.

Stop! Think Fraud campaign website

Action Fraud
24/7 live cyber crime reporting for businesses, run by the National Fraud & Cyber Crime Reporting Centre.

Action Fraud website

Take Five to Stop Fraud
Take Five is a national campaign offering straightforward and impartial advice to help everyone protect themselves against fraud.

Take Five to Stop Fraud website

The Little Guide to...
The "Little" series of books and videos explain some of the most common scams and give advice on how to avoid falling victim to them.

Metropolitan Police website

For more information visit

www.visa.co.uk/empowerahead/fraud-prevention-toolkit

Disclaimer

Case studies, comparisons, statistics, research, and recommendations are provided "AS IS' and intended for information purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.

Sources

1. New Visa research, based on 1,000 senior SMB decision makers in the UK. Due to be published end of November 24
2. https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.20491.html
3. https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps570-million-stolen-fraudsters-in-first-half-2024
4. https://usa.visa.com/visa-everywhere/blog/bdp/2022/06/15/what-every-merchant-1655330664445.html
5. https://investor.visa.com/news/news-details/2023/Visa-Research-Highlights-Emerging-Fraud-Schemes-in-Retail-and-eCommerce/default.aspx
6. https://navigate.visa.com/europe/security/what-were-the-major-fraud-and-security-threats-in-2022/