POL00448122

Security top tips

Please remember to read the Post Office Security Operations Guide for detailed security guidelines, available on:

- Branch Hub (log in required)
- Horizon Help [F9: Other Help (Including Security) / F3 Security Operations]
- Grapevine website

Here are some top tips to help keep you and your branch safe.

Be vigilant at opening times

- Check the outside of the building and remain vigilant at all times
- Never enter the premises if there are signs of a break in. Contact the Police and wait for them to arrive
- When entering the building, lock the door behind you before turning off the alarm

Keep your cash safe

- Keep cash at the counter to a minimum and within the limits allowed: no more than £1,000 for a screenless counter and no more than £2,500 for a fortress counter
- In open plan positions, remember to use the cash funding units, (BidiSafe, Cashette, RollerCash or Drop Safe)
- Secure the cash funding unit key in the main safe throughout the day

Cash collections and deliveries

- Tend to the CViT delivery as soon as you have finished serving your existing customer
- Secure all accepted remittances in the safe for at least 30 minutes
- Remember to replenish the ATM outside of business hours and away from public view
- Try to vary the day and time that you replenish the ATM

Security Equipment

- Make sure all alarm systems are set correctly
- Ensure safes are alarmed, closed and locked when not in use, and the keys withdrawn and secured safely out of sight throughout the day
- Where installed, make use of time delay equipment

Closing your branch securely

- Avoid opening the safe during the 30-minute period before branch closure
- Once you have secured all your cash and stock in the Post Office safe, ensure the Bidi safe, and counter drawers are left open to show they are empty

Remember! Remain vigilant at all times and report any suspicious activity to Post Office Grapevine. If you are in imminent danger, please call **999**.

Register at **grapevine.co.uk** to receive email and text alerts of suspicious activity reported in your locality.

POST OFFICE
GRAPEVINE
GRO

Strategic Partners: If your Post Office branch is located in a Strategic Partner store, such as WHSmith, Tesco, Co-Op, Blakemore etc, in addition to the Post Office security processes and procedures, you should also follow all the security processes and procedures issued by your company.

POL00448122

Admitting visitors

Please follow these steps before admitting visitors into any secure areas within your branch, or allowing anyone to do maintenance on the branch equipment:

- All visitors should have an appointment in advance and carry an official ID card
- Check the visitor's ID card before allowing them to enter
- For unannounced official visitors, including the police, Government department officials, fire brigade etc., contact the visitor's headquarters number to gain verification
- All visitors entering the secure area should complete an entry in the Branch Visitor Log

Note: The Branch Visitor Log tool is available on Branch Hub and retains a digital visitor log. Branches unable to access Branch Hub should use the manual printed sheet and retain these in branch.

- Visitors cannot be given unaccompanied access to Post Office devices, for example:
  - disconnecting PIN entry devices (PEDs)
  - opening Self Service Kiosks (SSKs) or ATMs
  - using any point of sale equipment (e.g. Horizon)
  - connecting unauthorised devices (e.g. USB sticks to the network or to access Horizon)

Important: If a Post Office visitor turns up without an appointment, you should verify their identity by calling Grapevine. A Visitor Verification table can be found in section 08 of the Post Office Security Operations Guide.

Remember: If you are suspicious in any way, refuse entry into the secure area and contact Grapevine to report your concerns.

PIN Entry Device (PED) security

All retailers that accept credit and debit cards for payment of goods or services are required to meet the Payment Card Industry - Data Security Standard (PCI DSS).

Visual inspection of PEDs need to be conducted every day, to help minimise the possibility of a customer using a device that has been tampered with. Check Horizon PIN pads, SSKs and ATMs, the key checks include:

- Checking for any visible damage to the device and/or cables
- Are there any extra cables or modules added?
- Have any labels appeared that could be hiding breaches in the casing?

Information on how to check a PED is available on Branch Hub.

In addition to the daily checks, a PCI Device Inspection declaration is made on Horizon each month to confirm the following:

- The PED make, model and serial numbers are correct
- Visual checks have been completed

Note: During the annual Payment Card Industry (PCI) audit, the PCI Device Inspection declaration needs to be produced as evidence that monthly tamper monitoring checks have been conducted.

Important: If you find the device has been tampered with, do not use it until the issue has been investigated and resolved. Report this to Grapevine as soon as possible.

Important: Please continue to retain your manual monthly PED Inspection Checklist in branch for 12 months from the date of completion as evidence for the PCI audit.

For details on the PCI Device Inspection declaration process, please refer to Section 12 Monthly Accounting.